

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

How to read the report | **Suppressing false positives** | **Getting Help: github issues**

Project: root project 'CoWorkInstaller'

cowork:CoWorkInstaller:26.10

Scan Information (show all):

- *dependency-check version*: 13.0.0
- *Report Generated On*: Mon, 28 Sep 2026 18:19:16 +0200
- *Dependencies Scanned*: 1302 (1243 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 125 (show)
- ...
- *NVD API Last Checked*: 2026-09-28T16:16:08Z
- *NVD API Last Modified*: 2026-09-02T21:13:38Z
- *NVD Cache Last Checked*: 2026-09-28T16:16:08Z
- *NVD Cache Last Modified*: 2026-09-02T21:13:38Z

Summary

Summary of Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Sever
Merlia-0.jar		pkg:maven/lib/Merlia@0	
ai.zip: ai.jar			
ai.zip: ai.jar: ai-skills-config-page.js			
ai.zip: ai.jar: aiprovider_config.js			
ai.zip: ai.jar: aiworkingpanel.js			
ai.zip: ai.jar: configuration.ai.skills.controller.js			
annotations-3.0.1.jar (shaded: com.google.code.findbugs:jsr305:3.0.1)		pkg:maven/com.google.code.findbugs/jsr305@3.0.1	
annotations-3.0.1.jar		pkg:maven/com.google.code.findbugs/annotations@3.0.1	
authentication.pam.zip: authentication.pam.jar			

authentication.pam.zip: jna.jar	cpe:2.3:a:oracle:java_se:5.18.1:*:*:*:*:*:*:* cpe:2.3:a:sun:java_se:5.18.1:*:*:*:*:*:*:*		
authentication.pam.zip: jna.jar: jnidispatch.dll			
authentication.pam.zip: jna.jar: jnidispatch.dll			
authentication.pam.zip: jna.jar: jnidispatch.dll			
authentication.product.zip: authentication.product.jar			
authentication.windows.zip: authentication.windows.jar			
authentication.windows.zip: caffeine.jar			
authentication.windows.zip: jna-platform.jar			
authentication.windows.zip: waffle-jna-jakarta.jar	cpe:2.3:a:4d:4d:3.5.1:*:*:*:*:*:*:*	pkg:maven/com.github.waffle/waffle-jna-jakarta@3.5.1	
bson.jar	cpe:2.3:a:mongodb:bson:5.9.2:*:*:*:*:*:*:*		
commons-logging.jar		pkg:maven/commons-logging/commons-logging@1.4.0	
configuration.zip: configuration.jar			
configuration.zip: configuration.jar: authenticationItemRenderer.directive.js			
configuration.zip: configuration.jar: authenticationRenderer.directive.js			
configuration.zip: configuration.jar: boolean.directive.js			
configuration.zip: configuration.jar: booleanButton.directive.js			
configuration.zip: configuration.jar: colorInput.directive.js			
configuration.zip: configuration.jar: controller.js			
configuration.zip: configuration.jar: datafactory.js			
configuration.zip: configuration.jar: fileUploadRenderer.directive.js			
configuration.zip: configuration.jar: filesystemFileInputOrUpload.directive.js			
configuration.zip: configuration.jar: filesystemInputButton.directive.js			
configuration.zip: configuration.jar: filesystemInputDirectory.directive.js			
configuration.zip: configuration.jar: filesystemInputFile.directive.js			

configuration.zip: configuration.jar: iconDropRenderer.directive.js			
configuration.zip: configuration.jar: inlinerenderer.directive.js			
configuration.zip: configuration.jar: keyLabelText.directive.js			
configuration.zip: configuration.jar: labelLink.directive.js			
configuration.zip: configuration.jar: labelText.directive.js			
configuration.zip: configuration.jar: licenseKeyItemRenderer.directive.js			
configuration.zip: configuration.jar: licenseKeyRenderer.directive.js			
configuration.zip: configuration.jar: listItemRenderer.directive.js			
configuration.zip: configuration.jar: logopreview.directive.js			
configuration.zip: configuration.jar: multiLineCode.directive.js			
configuration.zip: configuration.jar: multiLineText.directive.js			
configuration.zip: configuration.jar: multiLingualTextRenderer.directive.js			
configuration.zip: configuration.jar: passwordText.directive.js			
configuration.zip: configuration.jar: reloadCategoryTrigger.directive.js			
configuration.zip: configuration.jar: reloadSelectInputsTrigger.directive.js			
configuration.zip: configuration.jar: renderer.directive.js			
configuration.zip: configuration.jar: repoDbRenderer.directive.js			
configuration.zip: configuration.jar: repoFsRenderer.directive.js			
configuration.zip: configuration.jar: repositoryItemRenderer.directive.js			
configuration.zip: configuration.jar: repositoryRenderer.directive.js			
configuration.zip: configuration.jar: selectEditText.directive.js			
configuration.zip: configuration.jar: selectFilteredText.directive.js			
configuration.zip: configuration.jar: selectLanguageChooserRenderer.directive.js			
configuration.zip: configuration.jar: selectSimpleText.directive.js			

configuration.zip: configuration.jar: simpleDate.directive.js			
configuration.zip: configuration.jar: simpleSlider.directive.js			
configuration.zip: configuration.jar: simpleText.directive.js			
configuration.zip: configuration.jar: tableRenderer.directive.js			
configuration.zip: configuration.jar: treeRenderer.directive.js			
configuration.zip: configuration.jar: usersandgroupsselect.directive.js			
cowork.calls.zip: bc-fips.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.3:*:*:*:*:*:*:*		
cowork.calls.zip: bcpkix-fips.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.12:*:*:*:*:*:*:*		
cowork.calls.zip: bctls-fips.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.24:*:*:*:*:*:*:*		
cowork.calls.zip: bcutil-fips.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.7:*:*:*:*:*:*:*		
cowork.calls.zip: concentus.jar		pkg:maven/io.github.jaredmdobson/concentus@1.0.2	
cowork.calls.zip: config.jar			
cowork.calls.zip: cowork.calls.jar			
cowork.calls.zip: cowork.calls.jar: calltest.js			
cowork.calls.zip: cowork.calls.jar: coworkcallsactions.js			
cowork.calls.zip: cowork.calls.jar: coworkcallsettings.js			
cowork.calls.zip: cowork.calls.jar: coworkcallsfactory.js			
cowork.calls.zip: ice4j.jar	cpe:2.3:a:jitsi:jitsi:3.2.15.g6.da2:b08:*:*:*:*:*:*	pkg:maven/org.jitsi/ice4j@3.2-15-g6da2b08	
cowork.calls.zip: jicoco-config.jar	cpe:2.3:a:jitsi:jitsi:1.1.178.ga09.ed33:*:*:*:*:*:*:*	pkg:maven/org.jitsi/jicoco-config@1.1-178-ga09ed33	
cowork.calls.zip: jitsi-metaconfig.jar	cpe:2.3:a:jitsi:jitsi:1.0.17.g58971.d6:*:*:*:*:*:*:*	pkg:maven/org.jitsi/jitsi-metaconfig@1.0-17-g58971d6	
cowork.calls.zip: jitsi-utils.jar	cpe:2.3:a:jitsi:jitsi:1.0.150.g4.ab9:a3:*:*:*:*:*:*	pkg:maven/org.jitsi/jitsi-utils@1.0-150-	

	cpe:2.3:a:utils_project:utils:1.0.150.g4ab9:a3:*:*:*:*:*:*	g4ab9a3b	
cowork.calls.zip: kotlin-stdlib.jar	cpe:2.3:a:jetbrains:kotlin:2.4.20:*:*:*:*:*:*:*		
cowork.calls.zip: vosk.jar			
cowork.calls.zip: vosk.jar: libgcc_s_seh-1.dll			
cowork.calls.zip: vosk.jar: libstdc++-6.dll			
cowork.calls.zip: vosk.jar: libvosk.dll			
cowork.calls.zip: vosk.jar: libwinpthread-1.dll			
cowork.klipy.zip: cowork.klipy.jar			
cowork.klipy.zip: cowork.klipy.jar: coworkklipy.js			
cowork.klipy.zip: cowork.klipy.jar: klipygifselector.directive.js			
cowork.meetingrooms.zip: cowork.meetingrooms.jar			
cowork.meetingrooms.zip: cowork.meetingrooms.jar: coworkmeetingroom.js			
cowork.meetingrooms.zip: cowork.meetingrooms.jar: coworkmeetingroommoderator.js			
cowork.meetingrooms.zip: cowork.meetingrooms.jar: endofmeeting.js			
cowork.meetingrooms.zip: cowork.meetingrooms.jar: joinmeeting.js			
cowork.meetingrooms.zip: cowork.meetingrooms.jar: meetingrooms.maintenance.js			
cowork.tenor.zip: cowork.tenor.jar			
cowork.tenor.zip: cowork.tenor.jar: coworktenor.js			
cowork.tenor.zip: cowork.tenor.jar: tenorgifselector.directive.js			
cowork.waitingqueue.zip: cowork.waitingqueue.jar			
cowork.waitingqueue.zip: cowork.waitingqueue.jar: coworkwaitingqueue.dialog.js			
cowork.waitingqueue.zip: cowork.waitingqueue.jar: coworkwaitingqueue.indicator.js			
cowork.waitingqueue.zip: cowork.waitingqueue.jar: coworkwaitingqueue.js			
cowork.zip: cowork-javadoc.jar			
cowork.zip: cowork-javadoc.jar: jquery-3.7.1.min.js			
cowork.zip: cowork-javadoc.jar: jquery-ui.min.js			
cowork.zip: cowork-javadoc.jar: member-search-index.js			
cowork.zip: cowork-javadoc.jar: module-search-index.js			

cowork.zip: cowork-javadoc.jar: package-search-index.js			
cowork.zip: cowork-javadoc.jar: script.js			
cowork.zip: cowork-javadoc.jar: search-page.js			
cowork.zip: cowork-javadoc.jar: search.js			
cowork.zip: cowork-javadoc.jar: tag-search-index.js			
cowork.zip: cowork-javadoc.jar: type-search-index.js			
cowork.zip: cowork.jar			
cowork.zip: cowork.jar: MessageCreationChart.js			
cowork.zip: cowork.jar: cowork.diagnostics.js			
cowork.zip: cowork.jar: coworkcomponents.js			
cowork.zip: cowork.jar: coworkcontroller.js			
cowork.zip: cowork.jar: coworkconversation.js			
cowork.zip: cowork.jar: coworkfactory.js			
cowork.zip: cowork.jar: coworkinputbox.js			
cowork.zip: cowork.jar: coworkmodel.js			
cowork.zip: cowork.jar: coworksettingscontroller.js			
cowork.zip: cowork.jar: coworkstarredmessages.js			
cowork.zip: cowork.jar: inetmarkdown.js			
cowork.zip: cowork.jar: showreactionscontroller.js			
cowork.zip: cowork.jar: teamsettingscontroller.js			
dashboard.zip: dashboard.jar			
dashboard.zip: dashboard.jar: abstract-dashboard-widget.js			
dashboard.zip: dashboard.jar: dashboard-panel.js			
dashboard.zip: dashboard.jar: dashboard-settings.js			
dashboard.zip: dashboard.jar: dashboard-toolbar.js			
dashboard.zip: dashboard.jar: dashboard-widget-chart.js			
dashboard.zip: dashboard.jar: dashboard-widget-edit.js			
dashboard.zip: dashboard.jar: dashboard-widget-error.js			
dashboard.zip: dashboard.jar: dashboard-widget-image.js			
dashboard.zip: dashboard.jar: dashboard-widget-memo.js			
dashboard.zip: dashboard.jar: dashboard-widget-progress.js			
dashboard.zip: dashboard.jar: dashboard-widget-			

rating.js			
dashboard.zip: dashboard.jar: dashboard-widget-table.js			
dashboard.zip: dashboard.jar: dashboard-widget-trafficlight.js			
dashboard.zip: dashboard.jar: dashboard-widget-trend.js			
dashboard.zip: dashboard.jar: dashboard-widget-value.js			
dashboard.zip: dashboard.jar: dashboard-widget.js			
dashboard.zip: dashboard.jar: dashboard.js			
dashboard.zip: dashboard.jar: dashboardcontroller.js			
dashboard.zip: dashboard.jar: dashboardfactory.js			
dashboard.zip: dashboard.jar: ui-dashboard-bgimage.js			
dashboard.zip: dashboard.jar: ui-dashboard-colorpalettechooser.js			
dashboard.zip: dashboard.jar: ui-dashboard-integrations.js			
dashboard.zip: dashboard.jar: ui-dashboard-permissions.js			
dashboard.zip: dashboard.jar: ui-dashboard-tablecolumns.js			
dashboard.zip: dashboard.jar: ui-dashboard-trafficlightcolorrange.js			
dashboard.zip: dashboard.jar: ui-dashboard-valuehighlights.js			
dashboard.zip: dashboard.jar: user-selection.js			
dashboard.zip: dashboard.jar: widget-chooser.js			
dashboard.zip: dashboard.jar: widget-paste-area.js			
dashboard.zip: dashboard.jar: widget-placeholder.js			
dashboard.zip: dashboard.jar: widget-settings.js			
diagnostics.zip: diagnostics.jar			
diagnostics.zip: diagnostics.jar: MemoryPieChart.js			
diagnostics.zip: diagnostics.jar: MemoryUsageChart.js			
diagnostics.zip: diagnostics.jar: WebServerErrorChart.js			
diagnostics.zip: diagnostics.jar: benchmarkCtrl.js			
diagnostics.zip: diagnostics.jar: client-server.js			
diagnostics.zip: diagnostics.jar: contact-support-files.js			
diagnostics.zip: diagnostics.jar: contact-support-loader.js			

diagnostics.zip: diagnostics.jar: contact-support-panel.js			
diagnostics.zip: diagnostics.jar: contact-support-selection.js			
diagnostics.zip: diagnostics.jar: contact-support.js			
diagnostics.zip: diagnostics.jar: contactCtrl.js			
diagnostics.zip: diagnostics.jar: controller.js			
diagnostics.zip: diagnostics.jar: cpu.js			
diagnostics.zip: diagnostics.jar: cpuspeed.js			
diagnostics.zip: diagnostics.jar: directives.js			
diagnostics.zip: diagnostics.jar: errorHistoryChart.js			
diagnostics.zip: diagnostics.jar: global.js			
diagnostics.zip: diagnostics.jar: harddisk.js			
diagnostics.zip: diagnostics.jar: heapdumpCtrl.js			
diagnostics.zip: diagnostics.jar: informationCtrl.js			
diagnostics.zip: diagnostics.jar: intArrayUtils.js			
diagnostics.zip: diagnostics.jar: iospeed.js			
diagnostics.zip: diagnostics.jar: jobs.js			
diagnostics.zip: diagnostics.jar: logging.js			
diagnostics.zip: diagnostics.jar: memory.js			
diagnostics.zip: diagnostics.jar: overviewCtrl.js			
diagnostics.zip: diagnostics.jar: pde.diagnostics.js			
diagnostics.zip: diagnostics.jar: timeformat.js			
diagnostics.zip: diagnostics.jar: usermenu.js			
hamcrest-3.0.jar		pkg:maven/org.hamcrest/hamcrest@3.0	
help.zip: commons-beanutils.jar	cpe:2.3:a:apache:commons_beanutils:1.11.0:*:*:*:*:*:*:*	pkg:maven/commons-beanutils/commons-beanutils@1.11.0	
help.zip: commons-digester3.jar		pkg:maven/org.apache.commons/commons-digester3@3.2	
help.zip: help.jar			
help.zip: help.jar: ai-search.js			
help.zip: help.jar: app.js			
help.zip: help.jar: controller.js			

help.zip: help.jar: shared.factory.js			
help.zip: help.jar: shared.highlighter.js			
help.zip: jsoup.jar	cpe:2.3:a:jsoup:jsoup:1.23.1:*:*:*:*:*:*:*	pkg:maven/org.jsoup/jsoup@1.23.1	
htmlengine.zip: JWebEngine.jar			
htmlengine.zip: htmlengine.jar			
inetcore-26.10-tools.jar		pkg:maven/shared/inetcore@26.10	
inetcore-26.10.jar (shaded: com.inet.shared:inetcore:null)			
inetcore-26.10.jar		pkg:maven/shared/inetcore@26.10	
inetloggeradapter.jar			
jakarta.servlet-api.jar		pkg:maven/jakarta.servlet/jakarta.servlet-api@6.1.0	
jakarta.websocket-api.jar		pkg:maven/jakarta.websocket/jakarta.websocket-api@2.2.0	
jakarta.websocket-client-api.jar		pkg:maven/jakarta.websocket/jakarta.websocket-client-api@2.2.0	
java-25-jre-x64-linux.tar.gz: java-25-jre-x64-linux.tar: jrt-fs.jar	cpe:2.3:a:eclipse:platform:25.0.4:*:*:*:*:*:*:*		
jcip-annotations-1.0.jar		pkg:maven/net.jcip/jcip-annotations@1.0	
jlessc-1.16.jar		pkg:maven/de.inetsoftware/jlessc@1.16	
jsr305-3.0.2.jar		pkg:maven/com.google.code.findbugs/jsr305@3.0.2	
junit-4.13.2.jar	cpe:2.3:a:junit:junit4:4.13.2:*:*:*:*:*:*:*	pkg:maven/junit/junit@4.13.2	

junit-jupiter-6.1.3.jar		pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3	
junit-jupiter-api-6.1.3.jar		pkg:maven/org.junit.jupiter/junit-jupiter-api@6.1.3	
junit-jupiter-engine-6.1.3.jar		pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3	
junit-jupiter-params-6.1.3.jar		pkg:maven/org.junit.jupiter/junit-jupiter-params@6.1.3	
junit-platform-commons-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.platform/junit-platform-commons@6.1.3	
junit-platform-engine-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.platform/junit-platform-engine@6.1.3	
junit-platform-launcher-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.platform/junit-platform-launcher@6.1.3	
junit-platform-suite-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.platform/junit-platform-suite@6.1.3	
junit-platform-suite-api-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.platform/junit-platform-suite-api@6.1.3	
junit-platform-suite-engine-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.platform/junit-platform-suite-engine@6.1.3	
junit-vintage-engine-6.1.3.jar	cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:*	pkg:maven/org.junit.vintage/junit-vintage-engine@6.1.3	
mail.zip: angus-activation.jar		pkg:maven/org.eclipse.angus/angus-activation@2.0.3	
mail.zip: angus-mail.jar (shaded: org.eclipse.angus:angus-core:2.0.5)	cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:*	pkg:maven/org.eclipse.angus/angus-core@2.0.5	
mail.zip: angus-mail.jar (shaded: org.eclipse.angus:	cpe:2.3:a:eclipse:	pkg:maven/org.	

imap:2.0.5)	angus_mail:2.0.5:*:*:*:*:*:*:*	eclipse.angus/imap@2.0.5	
mail.zip: angus-mail.jar (shaded: org.eclipse.angus:logging-mailhandler:2.0.5)	cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:*	pkg:maven/org.eclipse.angus/logging-mailhandler@2.0.5	
mail.zip: angus-mail.jar (shaded: org.eclipse.angus:pop3:2.0.5)	cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:*	pkg:maven/org.eclipse.angus/pop3@2.0.5	
mail.zip: angus-mail.jar (shaded: org.eclipse.angus:smtp:2.0.5)	cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:*	pkg:maven/org.eclipse.angus/smtp@2.0.5	
mail.zip: angus-mail.jar	cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:*	pkg:maven/org.eclipse.angus/angus-mail@2.0.5	
mail.zip: bcjmail-fips.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.7:*:*:*:*:*:*:*		
mail.zip: bcpg-fips.jar	cpe:2.3:a:bouncycastle:bcpg-fips:2.1.13:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.13:*:*:*:*:*:*:* cpe:2.3:a:openpgp:openpgp:2.1.13:*:*:*:*:*:*:*		
mail.zip: jakarta.activation-api.jar		pkg:maven/jakarta.activation/jakarta.activation-api@2.1.4	
mail.zip: jakarta.mail-api.jar	cpe:2.3:a:eclipse:jakarta_mail:2.1.5:*:*:*:*:*:*:*	pkg:maven/jakarta.mail/jakarta.mail-api@2.1.5	
mail.zip: mail.jar			
mail.zip: mail.jar: smimeconfig.js			
maintenance.zip: maintenance-javadoc.jar			
maintenance.zip: maintenance-javadoc.jar: member-search-index.js			
maintenance.zip: maintenance-javadoc.jar: package-search-index.js			
maintenance.zip: maintenance-javadoc.jar: tag-search-index.js			
maintenance.zip: maintenance-javadoc.jar: type-search-index.js			
maintenance.zip: maintenance.jar			
maintenance.zip: maintenance.jar: controller.js			

maintenance.zip: maintenance.jar: controller.js			
maintenance.zip: maintenance.jar: controller.js			
maintenance.zip: maintenance.jar: controller.js			
maintenance.zip: maintenance.jar: controller.js			
maintenance.zip: maintenance.jar: filechooser.js			
maintenance.zip: maintenance.jar: loginmodification.js			
maintenance.zip: maintenance.jar: multieditusers.js			
mongodb-driver-core.jar			
mongodb-driver-sync.jar			
notification.zip: notification.jar			
notification.zip: notification.jar: notification.js			
notification.zip: notification.jar: notification_config.js			
notification.zip: notification.jar: notification_taskplanner.js			
notification.zip: notification.jar: targetrenderer.js			
opentest4j-1.3.0.jar		pkg:maven/org.opentest4j/opentest4j@1.3.0	
persistence.jar			
pluginstore.client.zip: pluginstore.client.jar			
pluginstore.client.zip: pluginstore.client.jar: controller.js			
pluginstore.client.zip: pluginstore.client.jar: pluginstorehelpcontroller.js			
pluginstore.client.zip: pluginstore.client.jar: publicstoreconfig.js			
pluginstore.client.zip: pluginstore.client.jar: storecontroller.js			
pluginstore.client.zip: pluginstore.client.jar: storedirectives.js			
pluginstore.client.zip: pluginstore.client.jar: storemodel.js			
remotegui.zip: angular-animate.jar		pkg:maven/org.webjars.npm/angular-animate@1.8.3	
remotegui.zip: angular-animate.jar: angular-animate.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular-animate.jar: angular-animate.min.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular-animate.jar: index.js			

remotegui.zip: angular-animate.jar: package.json			
remotegui.zip: angular-cookies.jar		pkg:maven/org.webjars.npm/angular-cookies@1.8.3	
remotegui.zip: angular-cookies.jar: angular-cookies.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular-cookies.jar: angular-cookies.min.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular-cookies.jar: index.js			
remotegui.zip: angular-cookies.jar: package.json			
remotegui.zip: angular-sanitize.jar		pkg:maven/org.webjars.npm/angular-sanitize@1.8.3	
remotegui.zip: angular-sanitize.jar: angular-sanitize.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular-sanitize.jar: angular-sanitize.min.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular-sanitize.jar: index.js			
remotegui.zip: angular-sanitize.jar: package.json			
remotegui.zip: angular.jar		pkg:maven/org.webjars.npm/angular@1.8.3	
remotegui.zip: angular.jar: angular.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular.jar: angular.min.js		pkg:javascript/angularjs@1.8.3	
remotegui.zip: angular.jar: index.js			
remotegui.zip: angular.jar: package.json			
remotegui.zip: codemirror.jar	cpe:2.3:a:codemirror:codemirror:5.65.21:*:*:*:*:*:*:*	pkg:maven/org.webjars.npm/codemirror@5.65.21	
remotegui.zip: codemirror.jar: CodeMirror.js			
remotegui.zip: codemirror.jar: ContentEditableInput.js			
remotegui.zip: codemirror.jar: Display.js			
remotegui.zip: codemirror.jar: Doc.js			
remotegui.zip: codemirror.jar: StringStream.js			
remotegui.zip: codemirror.jar: TextareaInput.js			

remotegui.zip: codemirror.jar: active-line.js

remotegui.zip: codemirror.jar: annotatescrollbar.js

remotegui.zip: codemirror.jar: anyword-hint.js

remotegui.zip: codemirror.jar: apl.js

remotegui.zip: codemirror.jar: asciiarmor.js

remotegui.zip: codemirror.jar: asn.1.js

remotegui.zip: codemirror.jar: asterisk.js

remotegui.zip: codemirror.jar: autorefresh.js

remotegui.zip: codemirror.jar: bidi.js

remotegui.zip: codemirror.jar: brace-fold.js

remotegui.zip: codemirror.jar: brainfuck.js

remotegui.zip: codemirror.jar: browser.js

remotegui.zip: codemirror.jar: change_measurement.js

remotegui.zip: codemirror.jar: changes.js

remotegui.zip: codemirror.jar: chunk.js

remotegui.zip: codemirror.jar: clike.js

remotegui.zip: codemirror.jar: clojure.js

remotegui.zip: codemirror.jar: closebrackets.js

remotegui.zip: codemirror.jar: closetag.js

remotegui.zip: codemirror.jar: cmake.js

remotegui.zip: codemirror.jar: cobol.js

remotegui.zip: codemirror.jar: codemirror-standalone.js

remotegui.zip: codemirror.jar: codemirror.js

remotegui.zip: codemirror.jar: codemirror.js

remotegui.zip: codemirror.jar: codemirror.node.js

remotegui.zip: codemirror.jar: coffeescript-lint.js

remotegui.zip: codemirror.jar: coffeescript.js

remotegui.zip: codemirror.jar: colorize.js

remotegui.zip: codemirror.jar: commands.js

remotegui.zip: codemirror.jar: comment-fold.js

remotegui.zip: codemirror.jar: comment.js

remotegui.zip: codemirror.jar: commonlisp.js

remotegui.zip: codemirror.jar: continuecomment.js

remotegui.zip: codemirror.jar: continuelist.js

remotegui.zip: codemirror.jar: crystal.js

remotegui.zip: codemirror.jar: css-hint.js			
remotegui.zip: codemirror.jar: css-lint.js			
remotegui.zip: codemirror.jar: css.js			
remotegui.zip: codemirror.jar: cypher.js			
remotegui.zip: codemirror.jar: d.js			
remotegui.zip: codemirror.jar: dart.js			
remotegui.zip: codemirror.jar: deleteNearSelection.js			
remotegui.zip: codemirror.jar: dialog.js			
remotegui.zip: codemirror.jar: diff.js			
remotegui.zip: codemirror.jar: django.js			
remotegui.zip: codemirror.jar: dockerfile.js			
remotegui.zip: codemirror.jar: document_data.js			
remotegui.zip: codemirror.jar: dom.js			
remotegui.zip: codemirror.jar: drop_events.js			
remotegui.zip: codemirror.jar: dtd.js			
remotegui.zip: codemirror.jar: dylan.js			
remotegui.zip: codemirror.jar: ebnf.js			
remotegui.zip: codemirror.jar: ecl.js			
remotegui.zip: codemirror.jar: eiffel.js			
remotegui.zip: codemirror.jar: elm.js			
remotegui.zip: codemirror.jar: emacs.js			
remotegui.zip: codemirror.jar: erlang.js			
remotegui.zip: codemirror.jar: event.js			
remotegui.zip: codemirror.jar: factor.js			
remotegui.zip: codemirror.jar: fcl.js			
remotegui.zip: codemirror.jar: feature_detection.js			
remotegui.zip: codemirror.jar: focus.js			
remotegui.zip: codemirror.jar: foldcode.js			
remotegui.zip: codemirror.jar: foldgutter.js			
remotegui.zip: codemirror.jar: forth.js			
remotegui.zip: codemirror.jar: fortran.js			
remotegui.zip: codemirror.jar: fromTextArea.js			
remotegui.zip: codemirror.jar: fullscreen.js			
remotegui.zip: codemirror.jar: gas.js			
remotegui.zip: codemirror.jar: gfm.js			

remotegui.zip: codemirror.jar: gherkin.js			
remotegui.zip: codemirror.jar: global_events.js			
remotegui.zip: codemirror.jar: go.js			
remotegui.zip: codemirror.jar: groovy.js			
remotegui.zip: codemirror.jar: gutters.js			
remotegui.zip: codemirror.jar: haml.js			
remotegui.zip: codemirror.jar: handlebars.js			
remotegui.zip: codemirror.jar: hardwrap.js			
remotegui.zip: codemirror.jar: haskell-literate.js			
remotegui.zip: codemirror.jar: haskell.js			
remotegui.zip: codemirror.jar: haxe.js			
remotegui.zip: codemirror.jar: highlight.js			
remotegui.zip: codemirror.jar: highlight_worker.js			
remotegui.zip: codemirror.jar: history.js			
remotegui.zip: codemirror.jar: html-hint.js			
remotegui.zip: codemirror.jar: html-lint.js			
remotegui.zip: codemirror.jar: htmlembedded.js			
remotegui.zip: codemirror.jar: htmlmixed.js			
remotegui.zip: codemirror.jar: http.js			
remotegui.zip: codemirror.jar: idl.js			
remotegui.zip: codemirror.jar: indent-fold.js			
remotegui.zip: codemirror.jar: indent.js			
remotegui.zip: codemirror.jar: input.js			
remotegui.zip: codemirror.jar: javascript-hint.js			
remotegui.zip: codemirror.jar: javascript-lint.js			
remotegui.zip: codemirror.jar: javascript.js			
remotegui.zip: codemirror.jar: jinja2.js			
remotegui.zip: codemirror.jar: json-lint.js			
remotegui.zip: codemirror.jar: jsx.js			
remotegui.zip: codemirror.jar: julia.js			
remotegui.zip: codemirror.jar: jump-to-line.js			
remotegui.zip: codemirror.jar: key_events.js			
remotegui.zip: codemirror.jar: keymap.js			
remotegui.zip: codemirror.jar: keynames.js			
remotegui.zip: codemirror.jar: legacy.js			

remotegui.zip: codemirror.jar: line_data.js			
remotegui.zip: codemirror.jar: line_numbers.js			
remotegui.zip: codemirror.jar: line_widget.js			
remotegui.zip: codemirror.jar: lint.js			
remotegui.zip: codemirror.jar: livescript.js			
remotegui.zip: codemirror.jar: loadmode.js			
remotegui.zip: codemirror.jar: lua.js			
remotegui.zip: codemirror.jar: main.js			
remotegui.zip: codemirror.jar: mark-selection.js			
remotegui.zip: codemirror.jar: mark_text.js			
remotegui.zip: codemirror.jar: markdown-fold.js			
remotegui.zip: codemirror.jar: markdown.js			
remotegui.zip: codemirror.jar: match-highlighter.js			
remotegui.zip: codemirror.jar: matchbrackets.js			
remotegui.zip: codemirror.jar: matchesonscrollbar.js			
remotegui.zip: codemirror.jar: matchtags.js			
remotegui.zip: codemirror.jar: mathematica.js			
remotegui.zip: codemirror.jar: mbox.js			
remotegui.zip: codemirror.jar: merge.js			
remotegui.zip: codemirror.jar: meta.js			
remotegui.zip: codemirror.jar: methods.js			
remotegui.zip: codemirror.jar: mirc.js			
remotegui.zip: codemirror.jar: misc.js			
remotegui.zip: codemirror.jar: mllike.js			
remotegui.zip: codemirror.jar: mode_state.js			
remotegui.zip: codemirror.jar: modelica.js			
remotegui.zip: codemirror.jar: modes.js			
remotegui.zip: codemirror.jar: mouse_events.js			
remotegui.zip: codemirror.jar: movement.js			
remotegui.zip: codemirror.jar: mscgen.js			
remotegui.zip: codemirror.jar: multiplex.js			
remotegui.zip: codemirror.jar: multiplex_test.js			
remotegui.zip: codemirror.jar: mumps.js			
remotegui.zip: codemirror.jar: nginx.js			
remotegui.zip: codemirror.jar: nsis.js			

remotegui.zip: codemirror.jar: ntriples.js

remotegui.zip: codemirror.jar: octave.js

remotegui.zip: codemirror.jar: operation_group.js

remotegui.zip: codemirror.jar: operations.js

remotegui.zip: codemirror.jar: options.js

remotegui.zip: codemirror.jar: overlay.js

remotegui.zip: codemirror.jar: oz.js

remotegui.zip: codemirror.jar: package.json

remotegui.zip: codemirror.jar: panel.js

remotegui.zip: codemirror.jar: pascal.js

remotegui.zip: codemirror.jar: pegjs.js

remotegui.zip: codemirror.jar: perl.js

remotegui.zip: codemirror.jar: php.js

remotegui.zip: codemirror.jar: pig.js

remotegui.zip: codemirror.jar: placeholder.js

remotegui.zip: codemirror.jar: pos.js

remotegui.zip: codemirror.jar: position_measurement.js

remotegui.zip: codemirror.jar: powershell.js

remotegui.zip: codemirror.jar: properties.js

remotegui.zip: codemirror.jar: protobuf.js

remotegui.zip: codemirror.jar: pug.js

remotegui.zip: codemirror.jar: puppet.js

remotegui.zip: codemirror.jar: python.js

remotegui.zip: codemirror.jar: q.js

remotegui.zip: codemirror.jar: r.js

remotegui.zip: codemirror.jar: rollup.config.js

remotegui.zip: codemirror.jar: rpm.js

remotegui.zip: codemirror.jar: rst.js

remotegui.zip: codemirror.jar: ruby.js

remotegui.zip: codemirror.jar: rulers.js

remotegui.zip: codemirror.jar: runmode-standalone.js

remotegui.zip: codemirror.jar: runmode-standalone.js

remotegui.zip: codemirror.jar: runmode.js

remotegui.zip: codemirror.jar: runmode.node.js

remotegui.zip: codemirror.jar: runmode.node.js

remotegui.zip: codemirror.jar: rust.js			
remotegui.zip: codemirror.jar: sas.js			
remotegui.zip: codemirror.jar: sass.js			
remotegui.zip: codemirror.jar: saw_special_spans.js			
remotegui.zip: codemirror.jar: scheme.js			
remotegui.zip: codemirror.jar: scroll_events.js			
remotegui.zip: codemirror.jar: scrollbars.js			
remotegui.zip: codemirror.jar: scrolling.js			
remotegui.zip: codemirror.jar: scrollpastend.js			
remotegui.zip: codemirror.jar: search.js			
remotegui.zip: codemirror.jar: searchcursor.js			
remotegui.zip: codemirror.jar: selection-pointer.js			
remotegui.zip: codemirror.jar: selection.js			
remotegui.zip: codemirror.jar: selection.js			
remotegui.zip: codemirror.jar: selection_updates.js			
remotegui.zip: codemirror.jar: shell.js			
remotegui.zip: codemirror.jar: show-hint.js			
remotegui.zip: codemirror.jar: sieve.js			
remotegui.zip: codemirror.jar: simple.js			
remotegui.zip: codemirror.jar: simplescrollbars.js			
remotegui.zip: codemirror.jar: slim.js			
remotegui.zip: codemirror.jar: smalltalk.js			
remotegui.zip: codemirror.jar: smarty.js			
remotegui.zip: codemirror.jar: solr.js			
remotegui.zip: codemirror.jar: soy.js			
remotegui.zip: codemirror.jar: spans.js			
remotegui.zip: codemirror.jar: sparql.js			
remotegui.zip: codemirror.jar: spreadsheet.js			
remotegui.zip: codemirror.jar: sql-hint.js			
remotegui.zip: codemirror.jar: sql.js			
remotegui.zip: codemirror.jar: stex.js			
remotegui.zip: codemirror.jar: stylus.js			
remotegui.zip: codemirror.jar: sublime.js			
remotegui.zip: codemirror.jar: swift.js			
remotegui.zip: codemirror.jar: tcl.js			

remotegui.zip: codemirror.jar: tern.js

remotegui.zip: codemirror.jar: textile.js

remotegui.zip: codemirror.jar: tiddlywiki.js

remotegui.zip: codemirror.jar: tiki.js

remotegui.zip: codemirror.jar: toml.js

remotegui.zip: codemirror.jar: tornado.js

remotegui.zip: codemirror.jar: trailingspace.js

remotegui.zip: codemirror.jar: troff.js

remotegui.zip: codemirror.jar: ttcn-cfg.js

remotegui.zip: codemirror.jar: ttcn.js

remotegui.zip: codemirror.jar: turtle.js

remotegui.zip: codemirror.jar: twig.js

remotegui.zip: codemirror.jar: update_display.js

remotegui.zip: codemirror.jar: update_line.js

remotegui.zip: codemirror.jar: update_lines.js

remotegui.zip: codemirror.jar: utils.js

remotegui.zip: codemirror.jar: utils_line.js

remotegui.zip: codemirror.jar: vb.js

remotegui.zip: codemirror.jar: vbscript.js

remotegui.zip: codemirror.jar: velocity.js

remotegui.zip: codemirror.jar: verilog.js

remotegui.zip: codemirror.jar: vhdl.js

remotegui.zip: codemirror.jar: view_tracking.js

remotegui.zip: codemirror.jar: vim.js

remotegui.zip: codemirror.jar: vue.js

remotegui.zip: codemirror.jar: wast.js

remotegui.zip: codemirror.jar: webidl.js

remotegui.zip: codemirror.jar: widgets.js

remotegui.zip: codemirror.jar: worker.js

remotegui.zip: codemirror.jar: xml-fold.js

remotegui.zip: codemirror.jar: xml-hint.js

remotegui.zip: codemirror.jar: xml.js

remotegui.zip: codemirror.jar: xquery.js

remotegui.zip: codemirror.jar: yacas.js

remotegui.zip: codemirror.jar: yaml-frontmatter.js

remotegui.zip: codemirror.jar: yaml-lint.js			
remotegui.zip: codemirror.jar: yaml.js			
remotegui.zip: codemirror.jar: z80.js			
remotegui.zip: crypto-js.jar		pkg:maven/org.webjars.npm/crypto-js@4.2.0	
remotegui.zip: crypto-js.jar: aes.js			
remotegui.zip: crypto-js.jar: blowfish.js			
remotegui.zip: crypto-js.jar: cipher-core.js			
remotegui.zip: crypto-js.jar: core.js			
remotegui.zip: crypto-js.jar: crypto-js.js			
remotegui.zip: crypto-js.jar: enc-base64.js			
remotegui.zip: crypto-js.jar: enc-base64url.js			
remotegui.zip: crypto-js.jar: enc-hex.js			
remotegui.zip: crypto-js.jar: enc-latin1.js			
remotegui.zip: crypto-js.jar: enc-utf16.js			
remotegui.zip: crypto-js.jar: enc-utf8.js			
remotegui.zip: crypto-js.jar: evpkdf.js			
remotegui.zip: crypto-js.jar: format-hex.js			
remotegui.zip: crypto-js.jar: format-openssl.js			
remotegui.zip: crypto-js.jar: hmac-md5.js			
remotegui.zip: crypto-js.jar: hmac-ripemd160.js			
remotegui.zip: crypto-js.jar: hmac-sha1.js			
remotegui.zip: crypto-js.jar: hmac-sha224.js			
remotegui.zip: crypto-js.jar: hmac-sha256.js			
remotegui.zip: crypto-js.jar: hmac-sha3.js			
remotegui.zip: crypto-js.jar: hmac-sha384.js			
remotegui.zip: crypto-js.jar: hmac-sha512.js			
remotegui.zip: crypto-js.jar: hmac.js			
remotegui.zip: crypto-js.jar: index.js			
remotegui.zip: crypto-js.jar: lib-typedarrays.js			
remotegui.zip: crypto-js.jar: md5.js			
remotegui.zip: crypto-js.jar: mode-cfb.js			
remotegui.zip: crypto-js.jar: mode-ctr-gladman.js			
remotegui.zip: crypto-js.jar: mode-ctr.js			
remotegui.zip: crypto-js.jar: mode-ecb.js			

remotegui.zip: crypto-js.jar: mode-ofb.js			
remotegui.zip: crypto-js.jar: package.json			
remotegui.zip: crypto-js.jar: pad-ansix923.js			
remotegui.zip: crypto-js.jar: pad-iso10126.js			
remotegui.zip: crypto-js.jar: pad-iso97971.js			
remotegui.zip: crypto-js.jar: pad-nopadding.js			
remotegui.zip: crypto-js.jar: pad-pkcs7.js			
remotegui.zip: crypto-js.jar: pad-zeropadding.js			
remotegui.zip: crypto-js.jar: pbkdf2.js			
remotegui.zip: crypto-js.jar: rabbit-legacy.js			
remotegui.zip: crypto-js.jar: rabbit.js			
remotegui.zip: crypto-js.jar: rc4.js			
remotegui.zip: crypto-js.jar: ripemd160.js			
remotegui.zip: crypto-js.jar: sha1.js			
remotegui.zip: crypto-js.jar: sha224.js			
remotegui.zip: crypto-js.jar: sha256.js			
remotegui.zip: crypto-js.jar: sha3.js			
remotegui.zip: crypto-js.jar: sha384.js			
remotegui.zip: crypto-js.jar: sha512.js			
remotegui.zip: crypto-js.jar: tripledes.js			
remotegui.zip: crypto-js.jar: x64-core.js			
remotegui.zip: echarts.jar		pkg:maven/org.webjars.npm/echarts@6.1.0	
remotegui.zip: echarts.jar: echarts.min.js			
remotegui.zip: hugerte-languages.jar		pkg:maven/org.webjars.npm/hugerte-languages@1.0.10	
remotegui.zip: hugerte-languages.jar: ar.js			
remotegui.zip: hugerte-languages.jar: ar_SA.js			
remotegui.zip: hugerte-languages.jar: az.js			
remotegui.zip: hugerte-languages.jar: be.js			
remotegui.zip: hugerte-languages.jar: bg_BG.js			
remotegui.zip: hugerte-languages.jar: bn_BD.js			
remotegui.zip: hugerte-languages.jar: ca.js			
remotegui.zip: hugerte-languages.jar: cs.js			

remotegui.zip: hugerte-languages.jar: cy.js			
remotegui.zip: hugerte-languages.jar: da.js			
remotegui.zip: hugerte-languages.jar: de.js			
remotegui.zip: hugerte-languages.jar: el.js			
remotegui.zip: hugerte-languages.jar: eo.js			
remotegui.zip: hugerte-languages.jar: es.js			
remotegui.zip: hugerte-languages.jar: es_MX.js			
remotegui.zip: hugerte-languages.jar: et.js			
remotegui.zip: hugerte-languages.jar: eu.js			
remotegui.zip: hugerte-languages.jar: fa.js			
remotegui.zip: hugerte-languages.jar: fi.js			
remotegui.zip: hugerte-languages.jar: fr_FR.js			
remotegui.zip: hugerte-languages.jar: ga.js			
remotegui.zip: hugerte-languages.jar: gl.js			
remotegui.zip: hugerte-languages.jar: he_IL.js			
remotegui.zip: hugerte-languages.jar: hr.js			
remotegui.zip: hugerte-languages.jar: hu_HU.js			
remotegui.zip: hugerte-languages.jar: hy.js			
remotegui.zip: hugerte-languages.jar: id.js			
remotegui.zip: hugerte-languages.jar: is_IS.js			
remotegui.zip: hugerte-languages.jar: it.js			
remotegui.zip: hugerte-languages.jar: ja.js			
remotegui.zip: hugerte-languages.jar: ka_GE.js			
remotegui.zip: hugerte-languages.jar: kab.js			
remotegui.zip: hugerte-languages.jar: kk.js			
remotegui.zip: hugerte-languages.jar: ko_KR.js			
remotegui.zip: hugerte-languages.jar: ku.js			
remotegui.zip: hugerte-languages.jar: lt.js			
remotegui.zip: hugerte-languages.jar: lv.js			
remotegui.zip: hugerte-languages.jar: nb_NO.js			
remotegui.zip: hugerte-languages.jar: ne.js			
remotegui.zip: hugerte-languages.jar: nl.js			
remotegui.zip: hugerte-languages.jar: nl_BE.js			
remotegui.zip: hugerte-languages.jar: oc.js			
remotegui.zip: hugerte-languages.jar: pl.js			

remotegui.zip: hugerte-languages.jar: pt_BR.js			
remotegui.zip: hugerte-languages.jar: pt_PT.js			
remotegui.zip: hugerte-languages.jar: ro.js			
remotegui.zip: hugerte-languages.jar: ru.js			
remotegui.zip: hugerte-languages.jar: sk.js			
remotegui.zip: hugerte-languages.jar: sl_SI.js			
remotegui.zip: hugerte-languages.jar: sq.js			
remotegui.zip: hugerte-languages.jar: sr.js			
remotegui.zip: hugerte-languages.jar: sv_SE.js			
remotegui.zip: hugerte-languages.jar: ta.js			
remotegui.zip: hugerte-languages.jar: tg.js			
remotegui.zip: hugerte-languages.jar: th_TH.js			
remotegui.zip: hugerte-languages.jar: tr.js			
remotegui.zip: hugerte-languages.jar: ug.js			
remotegui.zip: hugerte-languages.jar: uk.js			
remotegui.zip: hugerte-languages.jar: uz.js			
remotegui.zip: hugerte-languages.jar: vi.js			
remotegui.zip: hugerte-languages.jar: zh_CN.js			
remotegui.zip: hugerte-languages.jar: zh_HK.js			
remotegui.zip: hugerte-languages.jar: zh_MO.js			
remotegui.zip: hugerte-languages.jar: zh_SG.js			
remotegui.zip: hugerte-languages.jar: zh_TW.js			
remotegui.zip: hugerte.jar		pkg:maven/org.webjars.npm/hugerte@1.0.12	
remotegui.zip: hugerte.jar: ar.js			
remotegui.zip: hugerte.jar: bg_BG.js			
remotegui.zip: hugerte.jar: ca.js			
remotegui.zip: hugerte.jar: content.inline.js			
remotegui.zip: hugerte.jar: content.inline.js			
remotegui.zip: hugerte.jar: content.inline.js			
remotegui.zip: hugerte.jar: content.inline.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			

remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: content.js			
remotegui.zip: hugerte.jar: cs.js			
remotegui.zip: hugerte.jar: da.js			
remotegui.zip: hugerte.jar: de.js			
remotegui.zip: hugerte.jar: el.js			
remotegui.zip: hugerte.jar: emojiimages.js			
remotegui.zip: hugerte.jar: emojiimages.min.js			
remotegui.zip: hugerte.jar: emojis.js			
remotegui.zip: hugerte.jar: emojis.min.js			
remotegui.zip: hugerte.jar: en.js			
remotegui.zip: hugerte.jar: es.js			
remotegui.zip: hugerte.jar: eu.js			
remotegui.zip: hugerte.jar: fa.js			
remotegui.zip: hugerte.jar: fi.js			
remotegui.zip: hugerte.jar: fr_FR.js			
remotegui.zip: hugerte.jar: he_IL.js			
remotegui.zip: hugerte.jar: hi.js			
remotegui.zip: hugerte.jar: hr.js			
remotegui.zip: hugerte.jar: hu_HU.js			
remotegui.zip: hugerte.jar: hugerte.js		pkg:javascript/DOMPurify@3.4.11	
remotegui.zip: hugerte.jar: hugerte.min.js		pkg:javascript/DOMPurify@3.4.11	
remotegui.zip: hugerte.jar: icons.js			
remotegui.zip: hugerte.jar: icons.min.js			
remotegui.zip: hugerte.jar: id.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			

remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: index.js			
remotegui.zip: hugerte.jar: it.js			
remotegui.zip: hugerte.jar: ja.js			
remotegui.zip: hugerte.jar: kk.js			
remotegui.zip: hugerte.jar: ko_KR.js			
remotegui.zip: hugerte.jar: model.js			
remotegui.zip: hugerte.jar: model.min.js			

remotegui.zip: hugerte.jar: ms.js			
remotegui.zip: hugerte.jar: nb_NO.js			
remotegui.zip: hugerte.jar: nl.js			
remotegui.zip: hugerte.jar: package.json			
remotegui.zip: hugerte.jar: pl.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			
remotegui.zip: hugerte.jar: plugin.js			

remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: plugin.min.js			
remotegui.zip: hugerte.jar: pt_BR.js			
remotegui.zip: hugerte.jar: pt_PT.js			
remotegui.zip: hugerte.jar: ro.js			
remotegui.zip: hugerte.jar: ru.js			
remotegui.zip: hugerte.jar: sk.js			

remotegui.zip: hugerte.jar: skin.js			
remotegui.zip: hugerte.jar: skin.js			
remotegui.zip: hugerte.jar: skin.js			
remotegui.zip: hugerte.jar: skin.js			
remotegui.zip: hugerte.jar: skin.shadowdom.js			
remotegui.zip: hugerte.jar: skin.shadowdom.js			
remotegui.zip: hugerte.jar: skin.shadowdom.js			
remotegui.zip: hugerte.jar: skin.shadowdom.js			
remotegui.zip: hugerte.jar: sl_SI.js			
remotegui.zip: hugerte.jar: sv_SE.js			
remotegui.zip: hugerte.jar: th_TH.js			
remotegui.zip: hugerte.jar: theme.js		pkg:javascript/DOMPurify@3.4.11	
remotegui.zip: hugerte.jar: theme.min.js		pkg:javascript/DOMPurify@3.4.11	
remotegui.zip: hugerte.jar: tr.js			
remotegui.zip: hugerte.jar: uk.js			
remotegui.zip: hugerte.jar: vi.js			
remotegui.zip: hugerte.jar: zh_CN.js			
remotegui.zip: hugerte.jar: zh_TW.js			
remotegui.zip: jquery-ui.jar		pkg:maven/org.webjars/jquery-ui@1.14.2%2B1	
remotegui.zip: jquery-ui.jar: jquery-ui.js			
remotegui.zip: jquery-ui.jar: jquery-ui.min.js			
remotegui.zip: jquery-ui.jar: jquery.js			
remotegui.zip: jquery-ui.jar: package.json			
remotegui.zip: jquery.jar		pkg:javascript/jquery@2.2.4 pkg:maven/org.webjars/jquery@2.2.4	
remotegui.zip: jquery.jar: webjars-requirejs.js			
remotegui.zip: moment-timezone.jar		pkg:maven/org.webjars.npm/moment-timezone@0.6.2	
remotegui.zip: moment-timezone.jar: index.js			
remotegui.zip: moment-timezone.jar: moment-			

timezone-utils.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data-10-year-range.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data-10-year-range.min.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data-1970-2030.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data-1970-2030.min.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data-2012-2022.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data-2012-2022.min.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data.js			
remotegui.zip: moment-timezone.jar: moment-timezone-with-data.min.js			
remotegui.zip: moment-timezone.jar: moment-timezone.js			
remotegui.zip: moment-timezone.jar: moment-timezone.min.js			
remotegui.zip: moment-timezone.jar: package.json			
remotegui.zip: momentjs.jar		pkg:maven/org.webjars/momentjs@2.29.4	
remotegui.zip: momentjs.jar: af.js			
remotegui.zip: momentjs.jar: ar-dz.js			
remotegui.zip: momentjs.jar: ar-kw.js			
remotegui.zip: momentjs.jar: ar-ly.js			
remotegui.zip: momentjs.jar: ar-ma.js			
remotegui.zip: momentjs.jar: ar-sa.js			
remotegui.zip: momentjs.jar: ar-tn.js			
remotegui.zip: momentjs.jar: ar.js			
remotegui.zip: momentjs.jar: az.js			
remotegui.zip: momentjs.jar: be.js			
remotegui.zip: momentjs.jar: bg.js			
remotegui.zip: momentjs.jar: bm.js			
remotegui.zip: momentjs.jar: bn-bd.js			
remotegui.zip: momentjs.jar: bn.js			
remotegui.zip: momentjs.jar: bo.js			
remotegui.zip: momentjs.jar: br.js			

remotegui.zip: momentjs.jar: bs.js			
remotegui.zip: momentjs.jar: ca.js			
remotegui.zip: momentjs.jar: cs.js			
remotegui.zip: momentjs.jar: cv.js			
remotegui.zip: momentjs.jar: cy.js			
remotegui.zip: momentjs.jar: da.js			
remotegui.zip: momentjs.jar: de-at.js			
remotegui.zip: momentjs.jar: de-ch.js			
remotegui.zip: momentjs.jar: de.js			
remotegui.zip: momentjs.jar: dv.js			
remotegui.zip: momentjs.jar: el.js			
remotegui.zip: momentjs.jar: en-au.js			
remotegui.zip: momentjs.jar: en-ca.js			
remotegui.zip: momentjs.jar: en-gb.js			
remotegui.zip: momentjs.jar: en-ie.js			
remotegui.zip: momentjs.jar: en-il.js			
remotegui.zip: momentjs.jar: en-in.js			
remotegui.zip: momentjs.jar: en-nz.js			
remotegui.zip: momentjs.jar: en-sg.js			
remotegui.zip: momentjs.jar: eo.js			
remotegui.zip: momentjs.jar: es-do.js			
remotegui.zip: momentjs.jar: es-mx.js			
remotegui.zip: momentjs.jar: es-us.js			
remotegui.zip: momentjs.jar: es.js			
remotegui.zip: momentjs.jar: et.js			
remotegui.zip: momentjs.jar: eu.js			
remotegui.zip: momentjs.jar: fa.js			
remotegui.zip: momentjs.jar: fi.js			
remotegui.zip: momentjs.jar: fil.js			
remotegui.zip: momentjs.jar: fo.js			
remotegui.zip: momentjs.jar: fr-ca.js			
remotegui.zip: momentjs.jar: fr-ch.js			
remotegui.zip: momentjs.jar: fr.js			
remotegui.zip: momentjs.jar: fy.js			
remotegui.zip: momentjs.jar: ga.js			

remotegui.zip: momentjs.jar: gd.js			
remotegui.zip: momentjs.jar: gl.js			
remotegui.zip: momentjs.jar: gom-deva.js			
remotegui.zip: momentjs.jar: gom-latn.js			
remotegui.zip: momentjs.jar: gu.js			
remotegui.zip: momentjs.jar: he.js			
remotegui.zip: momentjs.jar: hi.js			
remotegui.zip: momentjs.jar: hr.js			
remotegui.zip: momentjs.jar: hu.js			
remotegui.zip: momentjs.jar: hy-am.js			
remotegui.zip: momentjs.jar: id.js			
remotegui.zip: momentjs.jar: is.js			
remotegui.zip: momentjs.jar: it-ch.js			
remotegui.zip: momentjs.jar: it.js			
remotegui.zip: momentjs.jar: ja.js			
remotegui.zip: momentjs.jar: jv.js			
remotegui.zip: momentjs.jar: ka.js			
remotegui.zip: momentjs.jar: kk.js			
remotegui.zip: momentjs.jar: km.js			
remotegui.zip: momentjs.jar: kn.js			
remotegui.zip: momentjs.jar: ko.js			
remotegui.zip: momentjs.jar: ku.js			
remotegui.zip: momentjs.jar: ky.js			
remotegui.zip: momentjs.jar: lb.js			
remotegui.zip: momentjs.jar: lo.js			
remotegui.zip: momentjs.jar: locales.js			
remotegui.zip: momentjs.jar: locales.min.js			
remotegui.zip: momentjs.jar: lt.js			
remotegui.zip: momentjs.jar: lv.js			
remotegui.zip: momentjs.jar: me.js			
remotegui.zip: momentjs.jar: mi.js			
remotegui.zip: momentjs.jar: mk.js			
remotegui.zip: momentjs.jar: ml.js			
remotegui.zip: momentjs.jar: mn.js			
remotegui.zip: momentjs.jar: moment-with-locales.js			

remotegui.zip: momentjs.jar: moment-with-locales.min.js			
remotegui.zip: momentjs.jar: moment.js			
remotegui.zip: momentjs.jar: moment.min.js			
remotegui.zip: momentjs.jar: mr.js			
remotegui.zip: momentjs.jar: ms-my.js			
remotegui.zip: momentjs.jar: ms.js			
remotegui.zip: momentjs.jar: mt.js			
remotegui.zip: momentjs.jar: my.js			
remotegui.zip: momentjs.jar: nb.js			
remotegui.zip: momentjs.jar: ne.js			
remotegui.zip: momentjs.jar: nl-be.js			
remotegui.zip: momentjs.jar: nl.js			
remotegui.zip: momentjs.jar: nn.js			
remotegui.zip: momentjs.jar: oc-lnc.js			
remotegui.zip: momentjs.jar: pa-in.js			
remotegui.zip: momentjs.jar: package.js			
remotegui.zip: momentjs.jar: package.json			
remotegui.zip: momentjs.jar: pl.js			
remotegui.zip: momentjs.jar: pt-br.js			
remotegui.zip: momentjs.jar: pt.js			
remotegui.zip: momentjs.jar: ro.js			
remotegui.zip: momentjs.jar: ru.js			
remotegui.zip: momentjs.jar: sd.js			
remotegui.zip: momentjs.jar: se.js			
remotegui.zip: momentjs.jar: si.js			
remotegui.zip: momentjs.jar: sk.js			
remotegui.zip: momentjs.jar: sl.js			
remotegui.zip: momentjs.jar: sq.js			
remotegui.zip: momentjs.jar: sr-cyrl.js			
remotegui.zip: momentjs.jar: sr.js			
remotegui.zip: momentjs.jar: ss.js			
remotegui.zip: momentjs.jar: sv.js			
remotegui.zip: momentjs.jar: sw.js			
remotegui.zip: momentjs.jar: ta.js			
remotegui.zip: momentjs.jar: te.js			

remotegui.zip: momentjs.jar: tests.js			
remotegui.zip: momentjs.jar: tet.js			
remotegui.zip: momentjs.jar: tg.js			
remotegui.zip: momentjs.jar: th.js			
remotegui.zip: momentjs.jar: tk.js			
remotegui.zip: momentjs.jar: tl-ph.js			
remotegui.zip: momentjs.jar: tlh.js			
remotegui.zip: momentjs.jar: tr.js			
remotegui.zip: momentjs.jar: tzl.js			
remotegui.zip: momentjs.jar: tzm-latn.js			
remotegui.zip: momentjs.jar: tzm.js			
remotegui.zip: momentjs.jar: ug-cn.js			
remotegui.zip: momentjs.jar: uk.js			
remotegui.zip: momentjs.jar: ur.js			
remotegui.zip: momentjs.jar: uz-latn.js			
remotegui.zip: momentjs.jar: uz.js			
remotegui.zip: momentjs.jar: vi.js			
remotegui.zip: momentjs.jar: webjars-requirejs.js			
remotegui.zip: momentjs.jar: x-pseudo.js			
remotegui.zip: momentjs.jar: yo.js			
remotegui.zip: momentjs.jar: zh-cn.js			
remotegui.zip: momentjs.jar: zh-hk.js			
remotegui.zip: momentjs.jar: zh-mo.js			
remotegui.zip: momentjs.jar: zh-tw.js			
remotegui.zip: remotegui.jar			
remotegui.zip: remotegui.jar: angular-websocket.js			
remotegui.zip: remotegui.jar: app.js			
remotegui.zip: remotegui.jar: app.js			
remotegui.zip: remotegui.jar: app.js			
remotegui.zip: remotegui.jar: app.js			
remotegui.zip: remotegui.jar: appbadge.service.js			
remotegui.zip: remotegui.jar: authInterceptor.service.js			
remotegui.zip: remotegui.jar: avatarcard.directive.js			
remotegui.zip: remotegui.jar: avatardetails.directive.js			
remotegui.zip: remotegui.jar: avatarimage.directive.js			

remotegui.zip: remotegui.jar: avatarimagedetails.directive.js			
remotegui.zip: remotegui.jar: basic.js			
remotegui.zip: remotegui.jar: bootstrap-colorpicker.js			
remotegui.zip: remotegui.jar: bootstrap-datetimepicker.js			
remotegui.zip: remotegui.jar: browsercheck.js			
remotegui.zip: remotegui.jar: changeavatar.js			
remotegui.zip: remotegui.jar: changeavatarcontroller.controller.js			
remotegui.zip: remotegui.jar: changeavatarservice.service.js			
remotegui.zip: remotegui.jar: chooser-color-popup.js			
remotegui.zip: remotegui.jar: clearreports.controller.js			
remotegui.zip: remotegui.jar: clipboardservice.js			
remotegui.zip: remotegui.jar: collapse.directive.js			
remotegui.zip: remotegui.jar: colorPicker.directive.js			
remotegui.zip: remotegui.jar: colorservice.js			
remotegui.zip: remotegui.jar: connectionstate.js			
remotegui.zip: remotegui.jar: controller.js			
remotegui.zip: remotegui.jar: controller.js			
remotegui.zip: remotegui.jar: controller.js			
remotegui.zip: remotegui.jar: controllerAbout.js			
remotegui.zip: remotegui.jar: controllerShortcuts.controller.js			
remotegui.zip: remotegui.jar: controllerUserTheme.controller.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: controllers.js			
remotegui.zip: remotegui.jar: currencyNumber.directive.js			
remotegui.zip: remotegui.jar: currencyValidator.directive.js			

remotegui.zip: remotegui.jar: customEmojiUploadConfigItemRenderer.directive.js			
remotegui.zip: remotegui.jar: customEmojiUploadConfigRenderer.directive.js			
remotegui.zip: remotegui.jar: customemojiupload.js			
remotegui.zip: remotegui.jar: dataservice.js			
remotegui.zip: remotegui.jar: dataservice.service.js			
remotegui.zip: remotegui.jar: datepicker-de.js			
remotegui.zip: remotegui.jar: debug.directive.js			
remotegui.zip: remotegui.jar: dialogservice.service.js			
remotegui.zip: remotegui.jar: directives.js			
remotegui.zip: remotegui.jar: dropdown.directive.js			
remotegui.zip: remotegui.jar: emojiModel.service.js			
remotegui.zip: remotegui.jar: emojiselector.directive.js			
remotegui.zip: remotegui.jar: env.js			
remotegui.zip: remotegui.jar: errorservice.js			
remotegui.zip: remotegui.jar: errorservice.service.js			
remotegui.zip: remotegui.jar: eventemitter.js			
remotegui.zip: remotegui.jar: filechooser.service.js			
remotegui.zip: remotegui.jar: filechooserservice.js			
remotegui.zip: remotegui.jar: fixNumber.directive.js			
remotegui.zip: remotegui.jar: fixNumberValidator.directive.js			
remotegui.zip: remotegui.jar: floatNumber.directive.js			
remotegui.zip: remotegui.jar: floatNumberValidator.directive.js			
remotegui.zip: remotegui.jar: globalactionservice.service.js			
remotegui.zip: remotegui.jar: guid.js			
remotegui.zip: remotegui.jar: hdField.directive.js			
remotegui.zip: remotegui.jar: hdMandatory.directive.js			
remotegui.zip: remotegui.jar: hdNeedchange.directive.js			
remotegui.zip: remotegui.jar: hdValidate.directive.js			
remotegui.zip: remotegui.jar: hdattachment.js			
remotegui.zip: remotegui.jar: hdfileupload.js			
remotegui.zip: remotegui.jar: helpservice.js			
remotegui.zip: remotegui.jar: hsimp.min.js			

remotegui.zip: remotegui.jar: hsimp.renderer.js			
remotegui.zip: remotegui.jar: html5modeurls.js			
remotegui.zip: remotegui.jar: htmleditor.directive.js			
remotegui.zip: remotegui.jar: htmleditorFactory.service.js			
remotegui.zip: remotegui.jar: htmleditorModel.service.js			
remotegui.zip: remotegui.jar: icons.js			
remotegui.zip: remotegui.jar: indexed-db.js			
remotegui.zip: remotegui.jar: initUsernameField.directive.js			
remotegui.zip: remotegui.jar: introduction.js			
remotegui.zip: remotegui.jar: jquery.fileupload.js			
remotegui.zip: remotegui.jar: keyservice.service.js			
remotegui.zip: remotegui.jar: kytos-attribute.js			
remotegui.zip: remotegui.jar: kytos-data.js			
remotegui.zip: remotegui.jar: kytos-draggable-listitem.js			
remotegui.zip: remotegui.jar: kytos-dropdown.js			
remotegui.zip: remotegui.jar: kytos-element.js			
remotegui.zip: remotegui.jar: kytos-i18n-placeholder.js			
remotegui.zip: remotegui.jar: kytos-i18n-title.js			
remotegui.zip: remotegui.jar: kytos-i18n.js			
remotegui.zip: remotegui.jar: kytos-on.js			
remotegui.zip: remotegui.jar: kytos-popover.js			
remotegui.zip: remotegui.jar: kytos-repeat.js			
remotegui.zip: remotegui.jar: kytos-src.js			
remotegui.zip: remotegui.jar: kytos.js			
remotegui.zip: remotegui.jar: localfilesystem.service.js			
remotegui.zip: remotegui.jar: locationservice.service.js			
remotegui.zip: remotegui.jar: modal.directive.js			
remotegui.zip: remotegui.jar: modalservice.js			
remotegui.zip: remotegui.jar: modalservice.service.js			
remotegui.zip: remotegui.jar: moduledragdrop.js			
remotegui.zip: remotegui.jar: navtabsoverflow.directive.js			
remotegui.zip: remotegui.jar: ng-hugerte.js			
remotegui.zip: remotegui.jar: ng-i18n.js			
remotegui.zip: remotegui.jar: number-util.js			

remotegui.zip: remotegui.jar: numberUtil.js			
remotegui.zip: remotegui.jar: numberValidatorUtil.factory.js			
remotegui.zip: remotegui.jar: ocLazyLoad.jsloader.js			
remotegui.zip: remotegui.jar: ocLazyLoad.min.js			
remotegui.zip: remotegui.jar: pageablenavbaractiondropdown.directive.js			
remotegui.zip: remotegui.jar: paged.filter.js			
remotegui.zip: remotegui.jar: pagination.directive.js			
remotegui.zip: remotegui.jar: piechart.directive.js			
remotegui.zip: remotegui.jar: popover.js			
remotegui.zip: remotegui.jar: pwa-service-worker.js			
remotegui.zip: remotegui.jar: pwa.js			
remotegui.zip: remotegui.jar: qrcode.min.js			
remotegui.zip: remotegui.jar: rangeSlider.directive.js			
remotegui.zip: remotegui.jar: rating.directive.js			
remotegui.zip: remotegui.jar: resizableDivider.js			
remotegui.zip: remotegui.jar: scrollabledropdownmenu.directive.js			
remotegui.zip: remotegui.jar: search-input.js			
remotegui.zip: remotegui.jar: search-panel.js			
remotegui.zip: remotegui.jar: selectInput.directive.js			
remotegui.zip: remotegui.jar: settings-ui-search.js			
remotegui.zip: remotegui.jar: settings-ui.js			
remotegui.zip: remotegui.jar: shadowLogger.factory.js			
remotegui.zip: remotegui.jar: sidenavigation.js			
remotegui.zip: remotegui.jar: takeoutDataController.controller.js			
remotegui.zip: remotegui.jar: takeoutDataFactory.factory.js			
remotegui.zip: remotegui.jar: takeoutDataModel.service.js			
remotegui.zip: remotegui.jar: timeInput.directive.js			
remotegui.zip: remotegui.jar: timeInputContainer.directive.js			
remotegui.zip: remotegui.jar: timeMeridiemContainer.directive.js			
remotegui.zip: remotegui.jar: toastservice.js			
remotegui.zip: remotegui.jar: translate.js			

remotegui.zip: remotegui.jar: ui-checkbox.js			
remotegui.zip: remotegui.jar: ui-chooser-color.js			
remotegui.zip: remotegui.jar: ui-chooser-file.js			
remotegui.zip: remotegui.jar: ui-group.js			
remotegui.zip: remotegui.jar: ui-input-multiline.js			
remotegui.zip: remotegui.jar: ui-input-number-fixed.js			
remotegui.zip: remotegui.jar: ui-input-number-float.js			
remotegui.zip: remotegui.jar: ui-input-password.js			
remotegui.zip: remotegui.jar: ui-input-search.js			
remotegui.zip: remotegui.jar: ui-input-text.js			
remotegui.zip: remotegui.jar: ui-input-unit.js			
remotegui.zip: remotegui.jar: ui-label.js			
remotegui.zip: remotegui.jar: ui-link.js			
remotegui.zip: remotegui.jar: ui-multi-property.js			
remotegui.zip: remotegui.jar: ui-property.js			
remotegui.zip: remotegui.jar: ui-radio-button.js			
remotegui.zip: remotegui.jar: ui-section.js			
remotegui.zip: remotegui.jar: ui-select-edit.js			
remotegui.zip: remotegui.jar: ui-select-filtered.js			
remotegui.zip: remotegui.jar: ui-select-options.js			
remotegui.zip: remotegui.jar: ui-slider.js			
remotegui.zip: remotegui.jar: unitFixNumber.directive.js			
remotegui.zip: remotegui.jar: unitFloatNumber.directive.js			
remotegui.zip: remotegui.jar: userservice.js			
remotegui.zip: remotegui.jar: usersorgroupsselection.js			
remotegui.zip: remotegui.jar: usestrict.js			
remotegui.zip: remotegui.jar: websitedownload.renderer.js			
remotegui.zip: remotegui.jar: websocketdataservice.js			
remotegui.zip: remotegui.jar: websocketkeepaliveworker.js			
remotegui.zip: remotegui.jar: windowdatarestore.js			
remotegui.zip: twemoji.jar		pkg:maven/lib/twemoji-null@1.0	
security.zip: security.jar			
setuplauncher.jar			

slf4j-api-2.0.18.jar		pkg:maven/org.slf4j/slf4j-api@2.0.18	
taskplanner.coworkmessage.zip: taskplanner.coworkmessage.jar			
taskplanner.zip: commons-cli.jar		pkg:maven/commons-cli/commons-cli@1.11.0	
taskplanner.zip: cron-utils.jar	cpe:2.3:a:cron-utils_project:cron-utils:9.2.1:*:*:*:*:*:*:* cpe:2.3:a:utils_project:utils:9.2.1:*:*:*:*:*:*:*	pkg:maven/com.cronutils/cron-utils@9.2.1	
taskplanner.zip: guava.jar	cpe:2.3:a:google:guava:33.5.0:*:*:*:*:*:*:*	pkg:maven/com.google.guava/guava@33.5.0-jre	
taskplanner.zip: taskplanner-javadoc.jar			
taskplanner.zip: taskplanner-javadoc.jar: member-search-index.js			
taskplanner.zip: taskplanner-javadoc.jar: package-search-index.js			
taskplanner.zip: taskplanner-javadoc.jar: tag-search-index.js			
taskplanner.zip: taskplanner-javadoc.jar: type-search-index.js			
taskplanner.zip: taskplanner.jar			
taskplanner.zip: taskplanner.jar: app.js			
taskplanner.zip: taskplanner.jar: boolean.directive.js			
taskplanner.zip: taskplanner.jar: colorField.directive.js			
taskplanner.zip: taskplanner.jar: controller.js			
taskplanner.zip: taskplanner.jar: factory.js			
taskplanner.zip: taskplanner.jar: filechooserAddonButton.directive.js			
taskplanner.zip: taskplanner.jar: model.js			
taskplanner.zip: taskplanner.jar: numberRange.directive.js			
taskplanner.zip: taskplanner.jar: numberWrapper.directive.js			
taskplanner.zip: taskplanner.jar: passwordTextField.directive.js			
taskplanner.zip: taskplanner.jar: renderer.directive.js			
taskplanner.zip: taskplanner.jar: simpleCurrencyField.directive.js			

taskplanner.zip: taskplanner.jar: simpleDateTimeField.directive.js			
taskplanner.zip: taskplanner.jar: simpleFileFolderField.directive.js			
taskplanner.zip: taskplanner.jar: simpleGroup.directive.js			
taskplanner.zip: taskplanner.jar: simpleLabel.directive.js			
taskplanner.zip: taskplanner.jar: simpleLink.directive.js			
taskplanner.zip: taskplanner.jar: simpleSelect.directive.js			
taskplanner.zip: taskplanner.jar: simpleTextField.directive.js			
taskplanner.zip: taskplanner.jar: stringTable.directive.js			
taskplanner.zip: taskplanner.jar: taskplanner_maintenance.js			
taskplanner.zip: taskplanner.jar: textAreaField.directive.js			
theme.zip: theme.jar			
usersandgroupsmanager.zip: usersandgroupsmanager.jar			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeAccountSettingsRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeBooleanRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeCommaSeparatedRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeCurrencyRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeDateRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeDoubleRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeHintRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeIntegerRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeLinkRenderer.directive.js			

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeLoginsRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeMembersRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeMultilineRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypePermissionRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeSelectRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeStayLoggedInSessionsRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeStringListRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeStringRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeTimeRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeTimerangeRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: membershipentry.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: membershiplist.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: nonmembershiplist.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: permissionCheckboxRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: permissionRadiobuttonRenderer.directive.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagercontroller.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerdetailscontroller.js			
usersandgroupsmanager.zip:			

usersandgroupsmanager.jar: usersandgroupsmanagerdialogcontroller.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerdirectives.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagereffectivepermissionscontroller.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerfactory.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagermodel.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerpredeletionwarning.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerrenderer.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerstatisticscontroller.js			
usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagertakeoutcontroller.js			
webserver.defender.zip: webserver.defender.jar			
webserver.zip: acme4j-client.jar		pkg:maven/org.shredzone.acme4j/acme4j-client@5.1.0	
webserver.zip: jetty-websocket-core-client.jar	cpe:2.3:a:eclipse:jetty:12.1.12:*:*:*:*:*:*:* cpe:2.3:a:jetty:jetty:12.1.12:*:*:*:*:*:*:* cpe:2.3:a:mortbay_jetty:jetty:12.1.12:*:*:*:*:*:*:*	pkg:maven/org.eclipse.jetty.websocket/jetty-websocket-core-client@12.1.12	
webserver.zip: jetty-websocket-core-server.jar	cpe:2.3:a:eclipse:jetty:12.1.12:*:*:*:*:*:*:* cpe:2.3:a:jetty:jetty:12.1.12:*:*:*:*:*:*:* cpe:2.3:a:jetty:jetty_http_server:12.1.12:*:*:*:*:*:*:* cpe:2.3:a:mortbay_jetty:jetty:12.1.12:*:*:*:*:*:*:*	pkg:maven/org.eclipse.jetty.websocket/jetty-websocket-core-server@12.1.12	
webserver.zip: jose4j.jar	cpe:2.3:a:jose4j_project:jose4j:0.9.6:*:*:*:*:*:*:*	pkg:maven/org.bitbucket.b_c/jose4j@0.9.6	
webserver.zip: webserver.jar			

Dependencies (vulnerable)

Merlia-0.jar

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/lib/Merlia/0
/ec818ab987afcd2d905984971f76a053ca107217/Merlia-0.jar
MD5: b151d3363029f809f49618ce97b8fc11
SHA1: ec818ab987afcd2d905984971f76a053ca107217
SHA256:cfe766dc3f0467f181c389a0a21323a408a674a54360fc6e3d46fdbb542ca453
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	Merlia-0	High
Vendor	gradle	artifactid	Merlia	Highest
Vendor	gradle	groupid	lib	Highest
Vendor	jar	package name	inet	Low
Vendor	jar	package name	tds	Low
Product	file	name	Merlia-0	High
Product	gradle	artifactid	Merlia	Highest
Product	jar	package name	tds	Low
Version	file	name	Merlia-0	Medium
Version	file	version	0	Medium
Version	gradle	version	0	Highest
Version	Manifest	driver-version	8.14	Medium

Identifiers

- pkg:maven/lib/Merlia@0 (*Confidence*:Highest)

ai.zip: ai.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller
/build/tmp/dependencies/i-net CoWork/plugins/ai.zip/ai.jar
MD5: caeea0663a720a4b1256c6a09b5cf7cf
SHA1: 4f168dc90e446e8234b1dc6d0a2e7ac3aaeb614f
SHA256:73dc37604a84b30b7557726ecdd8cb5291f06c28d5ec2f004d885f58c1c71652
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	ai	High
Vendor	jar	package name	ai	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	plugin	Low
Vendor	Manifest	built-date	2026-09-28 17:32	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	ai	High
Product	jar	package name	ai	Highest
Product	jar	package name	ai	Low
Product	jar	package name	plugin	Low
Product	Manifest	built-date	2026-09-28 17:32	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	ai	High
Product	Manifest	specification-title	ai	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

ai.zip: ai.jar: ai-skills-config-page.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/ai.zip/ai.jar/com/inet/plugin/ai/config/js/ai-skills-config-page.js
MD5: 621ee77f294b24af6428e59b31e1b998

SHA1: 9921a2b649875247150fa82662e8766ba2bc38c7
SHA256:e87e103a1c7f61be2b36d3a49111d1ad6f2aa9102df0bdce26bb1e36473ba319
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

ai.zip: ai.jar: aiprovider_config.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/ai.zip/ai.jar/com/inet/plugin/ai/structure/js/aiprovider_config.js
MD5: 68a9fc3064e6f6723ae905de550a5d9f
SHA1: 08b3e426d14a37a61ef955cfb70b06fbb02e016d
SHA256:14ccf885243643903eae46dc55aeabdbf6809f76852079b3cef945eb3706838d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

ai.zip: ai.jar: aiworkingpanel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/ai.zip/ai.jar/com/inet/plugin/ai/client/aiworkingpanel.js
MD5: 8b53a02567f9600fbdd8a3b9964434d7
SHA1: ba228e15518daba68bba59bd7e65e8a7bb2dcaef
SHA256:f9b3f83f731a8117347d5833c589a5b3e2037c01a60e8b403dc074726bb7b26d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

ai.zip: ai.jar: configuration.ai.skills.controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/ai.zip/ai.jar/com/inet/plugin/ai/config/js/configuration.ai.skills.controller.js
MD5: eab12da7182113b26463e371b6e3d2fe
SHA1: 6e54baaa9559502c540efd576a4007aedc608454
SHA256:be3b5635acec09a56f1d7da4a63f2bbcc8edcd6e62f28fc49253feb560aa2d4b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

annotations-3.0.1.jar (shaded: com.google.code.findbugs:jsr305:3.0.1)

Description:

JSR305 Annotations for Findbugs

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/com.google.code.findbugs/annotations/3.0.1/fc019a2216218990d64dfe756e7aa20f0069dea2/annotations-3.0.1.jar/META-INF/maven/com.google.code.findbugs/jsr305/pom.xml
MD5: d08567d16867a0b79bc8149683918452
SHA1: d04690f71f3393e23f30998d9534365274fa5f9f
SHA256:4170a761dc5bfd3981a8e6f7aab9e2acdce82d34fd5aa9bb11e3c090d25314ce
Referenced In Project/Scope: CoWorkInstaller:inetPlugin

Evidence

Type	Source	Name	Value	Confidence

Vendor	pom	artifactid	jsr305	Low
Vendor	pom	groupid	com.google.code.findbugs	Highest
Vendor	pom	name	FindBugs-jsr305	High
Vendor	pom	url	http://findbugs.sourceforge.net/	Highest
Product	pom	artifactid	jsr305	Highest
Product	pom	groupid	com.google.code.findbugs	Highest
Product	pom	name	FindBugs-jsr305	High
Product	pom	url	http://findbugs.sourceforge.net/	Medium
Version	pom	version	3.0.1	Highest

Identifiers

- pkg:maven/com.google.code.findbugs/jsr305@3.0.1 (*Confidence*:High)

annotations-3.0.1.jar

Description:

Annotation the FindBugs tool supports

License:

GNU Lesser Public License: http://www.gnu.org/licenses/lgpl.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/com.google.code.findbugs/annotations/3.0.1/fc019a2216218990d64dfe756e7aa20f0069dea2/annotations-3.0.1.jar
MD5: fc4f102f22ba4f1df3f1d7cc6b202152
SHA1: fc019a2216218990d64dfe756e7aa20f0069dea2
SHA256:6b47ff0a6de0ce17cbedc3abb0828ca5bce3009d53ea47b3723ff023c4742f79
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/de.inetsoftware/jlessc@1.16

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	annotations	High
Vendor	gradle	artifactid	annotations	Highest
Vendor	gradle	groupid	com.google.code.findbugs	Highest
Vendor	jar	package name	annotation	Highest
Vendor	jar	package name	annotations	Highest
Vendor	jar	package name	findbugs	Highest
Vendor	Manifest	bundle-	J2SE-1.5	Low

		requiredexecution		
Vendor	Manifest	bundle-symbolicname	findbugsAnnotations	Medium
Vendor	pom	artifactid	annotations	Low
Vendor	pom	developer email	Loskutov@gmx.de	Low
Vendor	pom	developer email	pugh at cs.umd.edu	Low
Vendor	pom	developer id	al	Medium
Vendor	pom	developer id	bp	Medium
Vendor	pom	developer name	Andrey Loskutov	Medium
Vendor	pom	developer name	Bill Pugh	Medium
Vendor	pom	developer name	Keith Lea	Medium
Vendor	pom	groupid	com.google.code.findbugs	Highest
Vendor	pom	name	FindBugs-Annotations	High
Vendor	pom	url	http://findbugs.sourceforge.net/	Highest
Product	file	name	annotations	High
Product	gradle	artifactid	annotations	Highest
Product	jar	package name	annotation	Highest
Product	jar	package name	annotations	Highest
Product	jar	package name	findbugs	Highest
Product	Manifest	Bundle-Name	FindBugs-Annotations	Medium
Product	Manifest	bundle-requiredexecution	J2SE-1.5	Low
Product	Manifest	bundle-symbolicname	findbugsAnnotations	Medium
Product	pom	artifactid	annotations	Highest
Product	pom	developer email	Loskutov@gmx.de	Low
Product	pom	developer email	pugh at cs.umd.edu	Low
Product	pom	developer id	al	Low
Product	pom	developer id	bp	Low
Product	pom	developer name	Andrey Loskutov	Low
Product	pom	developer name	Bill Pugh	Low
Product	pom	developer name	Keith Lea	Low
Product	pom	groupid	com.google.code.findbugs	Highest
Product	pom	name	FindBugs-Annotations	High
Product	pom	url	http://findbugs.sourceforge.net/	Medium
Version	file	version	3.0.1	High
Version	gradle	version	3.0.1	Highest

Version	Manifest	Bundle-Version	3.0.1	High
Version	pom	version	3.0.1	Highest

Identifiers

- pkg:maven/com.google.code.findbugs/annotations@3.0.1 (*Confidence*:High)

authentication.pam.zip: authentication.pam.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/authentication.pam.jar
MD5: 21797f1741bad58824945145b3bd3cfd
SHA1: d388c58eedef0dfa177c6de0e28562768fd3b896
SHA256:d3751c250a955dde5488bb88dcfb9586b6e56bbb55c55a58b5c4b09e332fd27b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	authentication.pam	High
Vendor	jar	package name	authentication	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	pam	Low
Vendor	Manifest	built-date	2026-09-28 17:24	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	authentication.pam	High
Product	jar	package name	authentication	Highest
Product	jar	package name	authentication	Low
Product	jar	package name	libpam	Low
Product	jar	package name	pam	Highest
Product	jar	package name	pam	Low

Product	Manifest	built-date	2026-09-28 17:24	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	authentication.pam	High
Product	Manifest	specification-title	authentication.pam	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

authentication.pam.zip: jna.jar

Description:

JNA Library

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/jna.jar
MD5: 97fcb12698f8c1e4eed897e5c490e098
SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
SHA256:9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jna	High
Vendor	jar	package name	jna	Highest
Vendor	jar	package name	jna	Low
Vendor	jar	package name	sun	Highest
Vendor	jar	package name	sun	Low
Vendor	jar (hint)	package name	oracle	Highest
Vendor	jar (hint)	package name	oracle	Low
Vendor	Manifest	automatic-module-name	com.sun.jna	Medium
Vendor	Manifest	bundle-activationpolicy	lazy	Low
Vendor	Manifest	bundle-category	jni	Low

Vendor	Manifest	bundle-nativecode	com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win32, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win32, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64; osname=win32, com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64;osname=win, com/sun/jna/w32ce-arm/jnidispatch.dll; processor=arm;osname=wince, com/sun/jna/sunos-x86/libjnidispatch.so; processor=x86; osname=sunos, com/sun/jna/sunos-x86-64/libjnidispatch.so; processor=x86-64; osname=sunos, com/sun/jna/sunos-sparc/libjnidispatch.so; processor=sparc; osname=sunos, com/sun/jna/sunos-sparcv9/libjnidispatch.so; processor=sparcv9; osname=sunos, com/sun/jna/aix-ppc/libjnidispatch.a; processor=ppc; osname=aix, com/sun/jna/aix-ppc64/libjnidispatch.a; processor=ppc64; osname=aix, com/sun/jna/linux-ppc/libjnidispatch.so; processor=ppc; osname=linux, com/sun/jna/linux-ppc64/libjnidispatch.so; processor=ppc64; osname=linux, com/sun/jna/linux-ppc64le/libjnidispatch.so; processor=ppc64le; osname=linux, com/sun/jna/linux-x86/libjnidispatch.so; processor=x86; osname=linux, com/sun/jna/linux-x86-64/libjnidispatch.so; processor=x86-64; osname=linux, com/sun/jna/linux-arm/libjnidispatch.so; processor=arm; osname=linux, com/sun/jna/linux-arm/libjnidispatch.so; processor=arm_le; osname=linux, com/sun/jna/linux-armel/libjnidispatch.so; processor=armel; osname=linux, com/sun/jna/linux-aarch64/libjnidispatch.so; processor=aarch64; osname=linux, com/sun/jna/linux-ia64/libjnidispatch.so; processor=ia64; osname=linux, com/sun/jna/linux-sparcv9/libjnidispatch.so; processor=sparcv9; osname=linux, com/sun/jna/linux-mips64el/libjnidispatch.so; processor=mips64el; osname=linux, com/sun/jna/linux-s390x/libjnidispatch.so; processor=S390x; osname=linux, com/sun/jna/linux-loongarch64/libjnidispatch.so; processor=loongarch64;osname=linux, com/sun/jna/linux-riscv64/libjnidispatch.so; processor=riscv64;osname=linux, com/sun/jna/dragonflybsd-x86-64/libjnidispatch.so; processor=x86-64;osname=dragonflybsd, com/sun/jna/freebsd-x86/libjnidispatch.so; processor=x86;osname=freebsd, com/sun/jna/freebsd-x86-64/libjnidispatch.so; processor=x86-64;osname=freebsd, com/sun/jna/freebsd-aarch64/libjnidispatch.so; processor=aarch64;osname=freebsd, com/sun/jna/freebsd-ppc64le/libjnidispatch.so; processor=ppc64le;osname=freebsd, com/sun/jna/freebsd-ppc64/libjnidispatch.so; processor=ppc64;osname=freebsd, com/sun	Low

			/jna/openbsd-x86/libjnidispatch.so; processor=x86;osname=openbsd, com/sun /jna/openbsd-x86-64/libjnidispatch.so; processor=x86-64;osname=openbsd, com /sun/jna/darwin-ppc/libjnidispatch.jnilib; osname=macosx;processor=ppc, com/sun /jna/darwin-ppc64/libjnidispatch.jnilib; osname=macosx;processor=ppc64, com/sun /jna/darwin-x86/libjnidispatch.jnilib; osname=macosx;processor=x86, com/sun /jna/darwin-x86-64/libjnidispatch.jnilib; osname=macosx;processor=x86-64, com /sun/jna/darwin-aarch64/libjnidispatch.jnilib; osname=macosx;processor=aarch64	
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.6	Low
Vendor	Manifest	bundle-symbolicname	com.sun.jna	Medium
Vendor	Manifest	Implementation-Vendor	JNA Development Team	High
Vendor	Manifest	specification-vendor	JNA Development Team	Low
Product	file	name	jna	High
Product	jar	package name	jna	Highest
Product	jar	package name	jna	Low
Product	jar	package name	library	Highest
Product	jar	package name	native	Highest
Product	jar	package name	sun	Highest
Product	jar	package name	win32	Highest
Product	Manifest	automatic-module-name	com.sun.jna	Medium
Product	Manifest	bundle-activationpolicy	lazy	Low
Product	Manifest	bundle-category	jni	Low
Product	Manifest	Bundle-Name	jna	Medium
Product	Manifest	bundle-nativecode	com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win32, com/sun/jna /win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win32, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64; osname=win32, com/sun/jna/win32-x86 /jnidispatch.dll; processor=x86;osname=win, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win, com/sun/jna /win32-aarch64/jnidispatch.dll; processor=aarch64;osname=win, com/sun /jna/w32ce-arm/jnidispatch.dll; processor=arm;osname=wince, com/sun/jna /sunos-x86/libjnidispatch.so; processor=x86; osname=sunos, com/sun/jna/sunos-x86-64 /libjnidispatch.so; processor=x86-64; osname=sunos, com/sun/jna/sunos-sparc /libjnidispatch.so; processor=sparc;	Low

			osname=sunos, com/sun/jna/sunos-sparcv9 /libjnidispatch.so; processor=sparcv9; osname=sunos, com/sun/jna/aix-ppc /libjnidispatch.a; processor=ppc; osname=aix, com/sun/jna/aix-ppc64 /libjnidispatch.a; processor=ppc64; osname=aix, com/sun/jna/linux-ppc /libjnidispatch.so; processor=ppc; osname=linux, com/sun/jna/linux-ppc64 /libjnidispatch.so; processor=ppc64; osname=linux, com/sun/jna/linux-ppc64le /libjnidispatch.so; processor=ppc64le; osname=linux, com/sun/jna/linux-x86 /libjnidispatch.so; processor=x86; osname=linux, com/sun/jna/linux-x86-64 /libjnidispatch.so; processor=x86-64; osname=linux, com/sun/jna/linux-arm /libjnidispatch.so; processor=arm; osname=linux, com/sun/jna/linux-arm /libjnidispatch.so; processor=arm_le; osname=linux, com/sun/jna/linux-armel /libjnidispatch.so; processor=armel; osname=linux, com/sun/jna/linux-aarch64 /libjnidispatch.so; processor=aarch64; osname=linux, com/sun/jna/linux-ia64 /libjnidispatch.so; processor=ia64; osname=linux, com/sun/jna/linux-sparcv9 /libjnidispatch.so; processor=sparcv9; osname=linux, com/sun/jna/linux-mips64el /libjnidispatch.so; processor=mips64el; osname=linux, com/sun/jna/linux-s390x /libjnidispatch.so; processor=S390x; osname=linux, com/sun/jna/linux-loongarch64/libjnidispatch.so; processor=loongarch64;osname=linux, com /sun/jna/linux-riscv64/libjnidispatch.so; processor=riscv64;osname=linux, com/sun /jna/dragonflybsd-x86-64/libjnidispatch.so; processor=x86-64;osname=dragonflybsd, com/sun/jna/freebsd-x86/libjnidispatch.so; processor=x86;osname=freebsd, com/sun /jna/freebsd-x86-64/libjnidispatch.so; processor=x86-64;osname=freebsd, com /sun/jna/freebsd-aarch64/libjnidispatch.so; processor=aarch64;osname=freebsd, com /sun/jna/freebsd-ppc64le/libjnidispatch.so; processor=ppc64le;osname=freebsd, com /sun/jna/freebsd-ppc64/libjnidispatch.so; processor=ppc64;osname=freebsd, com/sun /jna/openbsd-x86/libjnidispatch.so; processor=x86;osname=openbsd, com/sun /jna/openbsd-x86-64/libjnidispatch.so; processor=x86-64;osname=openbsd, com /sun/jna/darwin-ppc/libjnidispatch.jnilib; osname=macosx;processor=ppc, com/sun /jna/darwin-ppc64/libjnidispatch.jnilib; osname=macosx;processor=ppc64, com/sun /jna/darwin-x86/libjnidispatch.jnilib; osname=macosx;processor=x86, com/sun /jna/darwin-x86-64/libjnidispatch.jnilib; osname=macosx;processor=x86-64, com /sun/jna/darwin-aarch64/libjnidispatch.jnilib; osname=macosx;processor=aarch64	
Product	Manifest	bundle-requiredexecution	JavaSE-1.6	Low
Product	Manifest	bundle-	com.sun.jna	Medium

		symbolicname		
Product	Manifest	Implementation-Title	com.sun.jna	High
Product	Manifest	specification-title	Java Native Access (JNA)	Medium
Version	jar	package name	jna	Highest
Version	jar	package name	sun	Highest
Version	jar	package name	win32	Highest
Version	Manifest	Bundle-Version	5.18.1	High
Version	Manifest	Implementation-Version	5.18.1 (b0)	High

Related Dependencies

- authentication.windows.zip: jna.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/jna.jar
  - MD5: 97fcb12698f8c1e4eed897e5c490e098
  - SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
  - SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2
- cowork.calls.zip: jna.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jna.jar
  - MD5: 97fcb12698f8c1e4eed897e5c490e098
  - SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
  - SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2

Identifiers

- cpe:2.3:a:oracle:java_se:5.18.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:sun:java_se:5.18.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress

authentication.pam.zip: jna.jar: jnidispatch.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/jna.jar/com/sun/jna/win32-aarch64/jnidispatch.dll
MD5: 302945a811fd8e21bcdd5226c73b6f74
SHA1: 6b05e299ff2b3eb3b7b7aeac44263f715693607c
SHA256:b8f98be314234cf12b5b46c29652f70c0f6abb93ae19b63d3fe2692062aa699d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jnidispatch	High
Product	file	name	jnidispatch	High

Related Dependencies

- authentication.windows.zip: jna.jar: jnidispatch.dll
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /authentication.windows.zip/jna.jar/com/sun/jna/win32-aarch64/jnidispatch.dll
  - MD5: 302945a811fd8e21bcdd5226c73b6f74
  - SHA1: 6b05e299ff2b3eb3b7b7aeac44263f715693607c
  - SHA256: b8f98be314234cf12b5b46c29652f70c0f6abb93ae19b63d3fe2692062aa699d
- cowork.calls.zip: jna.jar: jnidispatch.dll
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jna.jar/com/sun/jna/win32-aarch64/jnidispatch.dll
  - MD5: 302945a811fd8e21bcdd5226c73b6f74
  - SHA1: 6b05e299ff2b3eb3b7b7aeac44263f715693607c
  - SHA256: b8f98be314234cf12b5b46c29652f70c0f6abb93ae19b63d3fe2692062aa699d

Identifiers

- **None**

authentication.pam.zip: jna.jar: jnidispatch.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller /build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/jna.jar/com/sun/jna/win32-x86-64 /jnidispatch.dll
MD5: 2d2475f1f026dd54e9f3e787ae4f81da
SHA1: 27ff882ac271db547aee520b38e3ba9aa91e136c
SHA256:5a7ff949f6d93d86491eb5b26b1cfc60051168a60622650224b89995ac420023
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jnidispatch	High
Product	file	name	jnidispatch	High

Related Dependencies

- authentication.windows.zip: jna.jar: jnidispatch.dll

- File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/jna.jar/com/sun/jna/win32-x86-64/jnidispatch.dll
- MD5: 2d2475f1f026dd54e9f3e787ae4f81da
- SHA1: 27ff882ac271db547aee520b38e3ba9aa91e136c
- SHA256: 5a7ff949f6d93d86491eb5b26b1cfc60051168a60622650224b89995ac420023

- cowork.calls.zip: jna.jar: jnidispatch.dll
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jna.jar/com/sun/jna/win32-x86-64/jnidispatch.dll
  - MD5: 2d2475f1f026dd54e9f3e787ae4f81da
  - SHA1: 27ff882ac271db547aee520b38e3ba9aa91e136c
  - SHA256: 5a7ff949f6d93d86491eb5b26b1cfc60051168a60622650224b89995ac420023

Identifiers

- **None**

authentication.pam.zip: jna.jar: jnidispatch.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/jna.jar/com/sun/jna/win32-x86/jnidispatch.dll
MD5: 0caa1ef75a807f9dde05084fa2219a5c
SHA1: 2f5e1cd82cde192905c7510ce99037b67d980640
SHA256:752d597cee7e95cb517327146bf42f124c0d6c0bc48b3ecc3b1b3b0531a52f44
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jnidispatch	High
Product	file	name	jnidispatch	High

Related Dependencies

- authentication.windows.zip: jna.jar: jnidispatch.dll
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/jna.jar/com/sun/jna/win32-x86/jnidispatch.dll
  - MD5: 0caa1ef75a807f9dde05084fa2219a5c
  - SHA1: 2f5e1cd82cde192905c7510ce99037b67d980640
  - SHA256: 752d597cee7e95cb517327146bf42f124c0d6c0bc48b3ecc3b1b3b0531a52f44
- cowork.calls.zip: jna.jar: jnidispatch.dll
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jna.jar/com/sun/jna/win32-x86/jnidispatch.dll
  - MD5: 0caa1ef75a807f9dde05084fa2219a5c
  - SHA1: 2f5e1cd82cde192905c7510ce99037b67d980640
  - SHA256: 752d597cee7e95cb517327146bf42f124c0d6c0bc48b3ecc3b1b3b0531a52f44

Identifiers

- **None**

authentication.product.zip: authentication.product.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.product.zip/authentication.product.jar
MD5: 7a07052d567d22ba176be5ba89484a16
SHA1: 6f20907695f91e67bc7fe02331f41c8bcdf2c761
SHA256:e8547ee8374fa3cca4d5e59bdb897b5f73949f6c3198efc1805c5986e9f90679
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	authentication.product	High
Vendor	jar	package name	authentication	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	product	Low
Vendor	Manifest	built-date	2026-09-28 17:29	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	authentication.product	High
Product	jar	package name	authentication	Highest
Product	jar	package name	authentication	Low
Product	jar	package name	product	Highest
Product	jar	package name	product	Low
Product	Manifest	built-date	2026-09-28 17:29	Low
Product	Manifest	implementation-group	shared	Low

Product	Manifest	Implementation-Title	authentication.product	High
Product	Manifest	specification-title	authentication.product	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

authentication.windows.zip: authentication.windows.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/authentication.windows.jar
MD5: bb569462c0df4950bf1451c67a27df8f
SHA1: 9b0c4c41adaee3bc3ba7d65fc6d5a8c607e1c01e
SHA256:486c44ad6186c8e5b29de53a8d8fc3da49c487665419819f5e7d4ff08d80c53e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	authentication.windows	High
Vendor	jar	package name	authentication	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	windows	Low
Vendor	Manifest	built-date	2026-09-28 17:25	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	authentication.windows	High
Product	jar	package name	authentication	Highest
Product	jar	package name	authentication	Low
Product	jar	package name	windows	Highest

Product	jar	package name	windows	Low
Product	Manifest	built-date	2026-09-28 17:25	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	authentication.windows	High
Product	Manifest	specification-title	authentication.windows	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

authentication.windows.zip: caffeine.jar

Description:

A high performance caching library

License:

https://www.apache.org/licenses/LICENSE-2.0

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/caffeine.jar
MD5: 7661b25999918646ec802846cc4c16bc
SHA1: 3646a0d1b1abe6a31f72f2237d9004d10a5be91d
SHA256:0311f9d5d9750aa2a1c11cbdba5a5cb7fec91c8870d6f179f324b3f5295b87dd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	caffeine	High
Vendor	jar	package name	benmanes	Highest
Vendor	jar	package name	benmanes	Low
Vendor	jar	package name	caffeine	Highest
Vendor	jar	package name	caffeine	Low
Vendor	jar	package name	github	Highest
Vendor	jar	package name	github	Low
Vendor	Manifest	automatic-module-name	com.github.benmanes.caffeine	Medium

Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-symbolicname	com.github.ben-manes.caffeine	Medium
Product	file	name	caffeine	High
Product	jar	package name	benmanes	Highest
Product	jar	package name	benmanes	Low
Product	jar	package name	cache	Low
Product	jar	package name	caffeine	Highest
Product	jar	package name	caffeine	Low
Product	jar	package name	github	Highest
Product	Manifest	automatic-module-name	com.github.benmanes.caffeine	Medium
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	Bundle-Name	com.github.ben-manes.caffeine	Medium
Product	Manifest	bundle-symbolicname	com.github.ben-manes.caffeine	Medium
Product	Manifest	Implementation-Title	A high performance caching library	High
Version	Manifest	build-jdk-spec	11	Low
Version	Manifest	Bundle-Version	3.1.6	High
Version	Manifest	Implementation-Version	3.1.6	High

Identifiers

- **None**

authentication.windows.zip: jna-platform.jar

Description:

JNA Platform Library

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/jna-platform.jar
MD5: a7af00779ec98bfe22dfb07b1532830d
SHA1: dd817f391efc492041c9ae91127527c13750a789
SHA256:ad14c1b1ec4f43d396231219dfa635ebf828f738eac9f890ea1bc07795892d9a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jna-platform	High
Vendor	jar	package name	jna	Highest
Vendor	jar	package name	jna	Low
Vendor	jar	package name	platform	Highest
Vendor	jar	package name	platform	Low
Vendor	jar	package name	sun	Highest
Vendor	jar	package name	sun	Low
Vendor	jar (hint)	package name	oracle	Highest
Vendor	jar (hint)	package name	oracle	Low
Vendor	Manifest	automatic-module-name	com.sun.jna.platform	Medium
Vendor	Manifest	bundle-category	jni	Low
Vendor	Manifest	bundle-requiredexecution	J2SE-1.4	Low
Vendor	Manifest	bundle-symbolicname	com.sun.jna.platform	Medium
Vendor	Manifest	Implementation-Vendor	JNA Development Team	High
Vendor	Manifest	specification-vendor	JNA Development Team	Low
Product	file	name	jna-platform	High
Product	jar	package name	jna	Highest
Product	jar	package name	jna	Low
Product	jar	package name	platform	Highest
Product	jar	package name	platform	Low
Product	jar	package name	sun	Highest
Product	jar	package name	win32	Low
Product	Manifest	automatic-module-name	com.sun.jna.platform	Medium
Product	Manifest	bundle-category	jni	Low
Product	Manifest	Bundle-Name	jna-platform	Medium
Product	Manifest	bundle-requiredexecution	J2SE-1.4	Low
Product	Manifest	bundle-symbolicname	com.sun.jna.platform	Medium
Product	Manifest	Implementation-Title	com.sun.jna	High

Product	Manifest	specification-title	Java Native Access (JNA)	Medium
Version	Manifest	Bundle-Version	5.18.1	High
Version	Manifest	Implementation-Version	5.18.1 (b0)	High

Identifiers

- **None**

authentication.windows.zip: waffle-jna-jakarta.jar

Description:

WAFFLE JNA Jakarta Pakage implementation

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/waffle-jna-jakarta.jar
MD5: 4292b31211ec75d0a54780009f620fd7
SHA1: a54b03b4de48b62188b183e04313092119f3e247
SHA256:e53d74bd6e09b543b97ccb7b5aff7dbdb1a9058066eafb9c2573c75adf254703
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	waffle-jna-jakarta	High
Vendor	jar	package name	waffle	Highest
Vendor	Manifest	automatic-module-name	waffle.jna.jakarta	Medium
Vendor	Manifest	build-jdk-spec	21	Low
Vendor	Manifest	copyright	2024	Low
Vendor	Manifest	git-revision	725e568c485ae01eddb2777e17e1c3f78955d4	Low
Vendor	Manifest	Implementation-Vendor	com.github.waffle	High
Vendor	Manifest	specification-vendor	com.github.waffle	Low
Vendor	pom	artifactid	waffle-jna-jakarta	Low
Vendor	pom	groupid	com.github.waffle	Highest
Vendor	pom	name	waffle-jna-jakarta	High
Vendor	pom	parent-artifactid	waffle	Low
Vendor	pom	url	https://waffle.github.io/waffle/	Highest

Product	file	name	waffle-jna-jakarta	High
Product	jar	package name	waffle	Highest
Product	Manifest	automatic-module-name	waffle.jna.jakarta	Medium
Product	Manifest	build-jdk-spec	21	Low
Product	Manifest	copyright	2024	Low
Product	Manifest	git-revision	725e568c485ae01eddb2777e17e1c3f78955d4	Low
Product	Manifest	Implementation-Title	waffle-jna-jakarta	High
Product	Manifest	specification-title	waffle-jna-jakarta	Medium
Product	pom	artifactid	waffle-jna-jakarta	Highest
Product	pom	groupid	com.github.waffle	Highest
Product	pom	name	waffle-jna-jakarta	High
Product	pom	parent-artifactid	waffle	Medium
Product	pom	url	https://waffle.github.io/waffle/	Medium
Version	Manifest	Implementation-Version	3.5.1	High
Version	pom	version	3.5.1	Highest

Identifiers

- pkg:maven/com.github.waffle/waffle-jna-jakarta@3.5.1 (*Confidence*:High)
- cpe:2.3:a:4d:4d:3.5.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress

bson.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/persistence/bson.jar
MD5: 6ea956f452018355a471c2d6fd3aff76
SHA1: ca1ea82fe2bb93f8b77717ee3513c001c986e115
SHA256:13d82f68daeaca951c036b400a30dcd4e4028ad287240ea6c7a975e94830acf0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bson	High
Vendor	jar	package name	bson	Highest
Vendor	jar	package name	bson	Low

Vendor	Manifest	automatic-module-name	org.mongodb.bson	Medium
Vendor	Manifest	bundle-symbolicname	org.mongodb.bson	Medium
Product	file	name	bson	High
Product	jar	package name	bson	Highest
Product	Manifest	automatic-module-name	org.mongodb.bson	Medium
Product	Manifest	Bundle-Name	bson	Medium
Product	Manifest	bundle-symbolicname	org.mongodb.bson	Medium
Version	Manifest	build-version	5.9.2	Medium
Version	Manifest	Bundle-Version	5.9.2	High

Identifiers

- cpe:2.3:a:mongodb:bson:5.9.2:*:*:*:*:*:*:* (*Confidence*:Medium) suppress

commons-logging.jar

Description:

Apache Commons Logging is a thin adapter allowing configurable bridging to other, well-known logging systems.

License:

https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/commons-logging.jar
MD5: 954e27d33e55e587a4694d5952a0c5c6
SHA1: e8f6313365dfa0580e49c58837afc8caa9b4ce05
SHA256:d175dbd751dd782a63bde28c7a039520e971f25e84b79c19b8435edc3603e0dc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	commons-logging	High
Vendor	jar	package name	apache	Highest
Vendor	jar	package name	commons	Highest
Vendor	jar	package name	logging	Highest

Vendor	Manifest	automatic-module-name	org.apache.commons.logging	Medium
Vendor	Manifest	build-jdk-spec	21	Low
Vendor	Manifest	bundle-docurl	https://commons.apache.org/proper/commons-logging/	Low
Vendor	Manifest	bundle-symbolicname	org.apache.commons.commons-logging	Medium
Vendor	Manifest	Implementation-Vendor	The Apache Software Foundation	High
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	specification-vendor	The Apache Software Foundation	Low
Vendor	pom	artifactid	commons-logging	Low
Vendor	pom	developer email	baliuka@apache.org	Low
Vendor	pom	developer email	costin@apache.org	Low
Vendor	pom	developer email	craigmcc@apache.org	Low
Vendor	pom	developer email	dennisl@apache.org	Low
Vendor	pom	developer email	donaldp@apache.org	Low
Vendor	pom	developer email	ggregory at apache.org	Low
Vendor	pom	developer email	morgand@apache.org	Low
Vendor	pom	developer email	rdonkin@apache.org	Low
Vendor	pom	developer email	rsitze@apache.org	Low
Vendor	pom	developer email	rwaldhoff@apache.org	Low
Vendor	pom	developer email	sanders@apache.org	Low
Vendor	pom	developer email	skitching@apache.org	Low
Vendor	pom	developer email	tn@apache.org	Low
Vendor	pom	developer id	baliuka	Medium
Vendor	pom	developer id	bstansberry	Medium
Vendor	pom	developer id	costin	Medium
Vendor	pom	developer id	craigmcc	Medium
Vendor	pom	developer id	dennisl	Medium
Vendor	pom	developer id	donaldp	Medium
Vendor	pom	developer id	ggregory	Medium
Vendor	pom	developer id	morgand	Medium
Vendor	pom	developer id	rdonkin	Medium
Vendor	pom	developer id	rsitze	Medium
Vendor	pom	developer id	rwaldhoff	Medium
Vendor	pom	developer id	sanders	Medium

Vendor	pom	developer id	skitching	Medium
Vendor	pom	developer id	tn	Medium
Vendor	pom	developer name	Brian Stansberry	Medium
Vendor	pom	developer name	Costin Manolache	Medium
Vendor	pom	developer name	Craig McClanahan	Medium
Vendor	pom	developer name	Dennis Lundberg	Medium
Vendor	pom	developer name	Gary Gregory	Medium
Vendor	pom	developer name	Juozas Baliuka	Medium
Vendor	pom	developer name	Morgan Delagrange	Medium
Vendor	pom	developer name	Peter Donald	Medium
Vendor	pom	developer name	Richard Sitze	Medium
Vendor	pom	developer name	Robert Burrell Donkin	Medium
Vendor	pom	developer name	Rodney Waldhoff	Medium
Vendor	pom	developer name	Scott Sanders	Medium
Vendor	pom	developer name	Simon Kitching	Medium
Vendor	pom	developer name	Thomas Neidhart	Medium
Vendor	pom	developer org	Apache	Medium
Vendor	pom	developer org	The Apache Software Foundation	Medium
Vendor	pom	developer org URL	https://www.apache.org/	Medium
Vendor	pom	groupid	commons-logging	Highest
Vendor	pom	name	Apache Commons Logging	High
Vendor	pom	parent-artifactid	commons-parent	Low
Vendor	pom	parent-groupid	org.apache.commons	Medium
Vendor	pom	url	https://commons.apache.org/proper/commons-logging/	Highest
Product	file	name	commons-logging	High
Product	jar	package name	apache	Highest
Product	jar	package name	commons	Highest
Product	jar	package name	logging	Highest
Product	Manifest	automatic-module-name	org.apache.commons.logging	Medium
Product	Manifest	build-jdk-spec	21	Low
Product	Manifest	bundle-docurl	https://commons.apache.org/proper/commons-logging/	Low
Product	Manifest	Bundle-Name	Apache Commons Logging	Medium
Product	Manifest	bundle-	org.apache.commons.commons-logging	Medium

		symbolicname		
Product	Manifest	Implementation-Title	Apache Commons Logging	High
Product	Manifest	multi-release	true	Low
Product	Manifest	specification-title	Apache Commons Logging	Medium
Product	pom	artifactid	commons-logging	Highest
Product	pom	developer email	baliuka@apache.org	Low
Product	pom	developer email	costin@apache.org	Low
Product	pom	developer email	craigmcc@apache.org	Low
Product	pom	developer email	dennisl@apache.org	Low
Product	pom	developer email	donaldp@apache.org	Low
Product	pom	developer email	ggregory at apache.org	Low
Product	pom	developer email	morgand@apache.org	Low
Product	pom	developer email	rdonkin@apache.org	Low
Product	pom	developer email	rsitze@apache.org	Low
Product	pom	developer email	rwaldhoff@apache.org	Low
Product	pom	developer email	sanders@apache.org	Low
Product	pom	developer email	skitching@apache.org	Low
Product	pom	developer email	tn@apache.org	Low
Product	pom	developer id	baliuka	Low
Product	pom	developer id	bstansberry	Low
Product	pom	developer id	costin	Low
Product	pom	developer id	craigmcc	Low
Product	pom	developer id	dennisl	Low
Product	pom	developer id	donaldp	Low
Product	pom	developer id	ggregory	Low
Product	pom	developer id	morgand	Low
Product	pom	developer id	rdonkin	Low
Product	pom	developer id	rsitze	Low
Product	pom	developer id	rwaldhoff	Low
Product	pom	developer id	sanders	Low
Product	pom	developer id	skitching	Low
Product	pom	developer id	tn	Low
Product	pom	developer name	Brian Stansberry	Low
Product	pom	developer name	Costin Manolache	Low
Product	pom	developer name	Craig McClanahan	Low

Product	pom	developer name	Dennis Lundberg	Low
Product	pom	developer name	Gary Gregory	Low
Product	pom	developer name	Juozas Baliuka	Low
Product	pom	developer name	Morgan Delagrange	Low
Product	pom	developer name	Peter Donald	Low
Product	pom	developer name	Richard Sitze	Low
Product	pom	developer name	Robert Burrell Donkin	Low
Product	pom	developer name	Rodney Waldhoff	Low
Product	pom	developer name	Scott Sanders	Low
Product	pom	developer name	Simon Kitching	Low
Product	pom	developer name	Thomas Neidhart	Low
Product	pom	developer org	Apache	Low
Product	pom	developer org	The Apache Software Foundation	Low
Product	pom	developer org URL	https://www.apache.org/	Low
Product	pom	groupid	commons-logging	Highest
Product	pom	name	Apache Commons Logging	High
Product	pom	parent-artifactid	commons-parent	Medium
Product	pom	parent-groupid	org.apache.commons	Medium
Product	pom	url	https://commons.apache.org/proper/commons-logging/	Medium
Version	Manifest	Bundle-Version	1.4.0	High
Version	Manifest	Implementation-Version	1.4.0	High
Version	pom	parent-version	1.4.0	Low
Version	pom	version	1.4.0	Highest

Identifiers

- pkg:maven/commons-logging/commons-logging@1.4.0 (*Confidence*:High)

configuration.zip: configuration.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar
MD5: d16b5e15f7526f396bc03e9992e260d3
SHA1: 8d2ad558a824fd4baca72c2612ab1d3a8179bebb

SHA256:361c3ff9b53da3ec431e321de74a017fe5e54c8f3b04c254c705cf165d8eebab
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	configuration	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	plugins	Low
Vendor	jar	package name	report	Low
Vendor	Manifest	built-date	2026-09-28 17:31	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	configuration	High
Product	jar	package name	config	Low
Product	jar	package name	plugins	Low
Product	jar	package name	report	Low
Product	Manifest	built-date	2026-09-28 17:31	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	configuration	High
Product	Manifest	specification-title	configuration	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

configuration.zip: configuration.jar: authenticationItemRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/authenticationItemRenderer.directive.js
MD5: aefb1a2a7d97d2df669e0545658c3e24
SHA1: 4a2a34c98fb71cf2dfa520bb02dc8baf0d0810f9
SHA256:c277d6842312394b3aa4ac0385e1c800c73dc0b2b0cd9696bc5f51293d859b29
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: authenticationRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/authenticationRenderer.directive.js
MD5: 08d42fd374d37fbb791917830a779fa8
SHA1: 3e7daea97fb445ace87c90fd3e9188690660d99d
SHA256:1719515423a8f8edcddfccb5519f22251afbedfd9de10bea76c99e461bd82929
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: boolean.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/boolean.directive.js
MD5: e281bd179c94019bdff388759a526f31
SHA1: 5f4be414c7db7b9c699a371bc3a84a945e1c13a3
SHA256:3e819332e6b9a66c5041ae377459a6b7d7f10fd94dd71ad85a3f8169fdab4f48
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: booleanButton.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/booleanButton.directive.js
MD5: dc5744f572a36fa29dc813914156944d
SHA1: 40a96829d9f498e1364fac7ec8bf8a626c4ac66c
SHA256:edf806317b3487f3998c758a4e56a0aa8bb08bfe38fd4b38c9ec68abbabf25f6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: colorInput.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/colorInput.directive.js
MD5: db9d1ee17d2b4f79813c66e8a52b8fcd
SHA1: 68e81a259a7bce7f49dbf629230020cdf0b01398
SHA256:1fff0ddf3d275467e77832ae82c55ffdebfbc4cc31aee0bfb31def6574f734ae
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/controller.js
MD5: 0dcc4e3a90917e61505df426f7d20f71
SHA1: abecca5a8567b134d6c49d8590344a82b7f2490f
SHA256:eb5dd123787faaf50c8ef51d240fae95c3999eb8740ef8b856ab9f630a23586c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: datafactory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/datafactory.js
MD5: d3ef8ef74e8a49df354e4bc43b028aed
SHA1: 0511810d8991fecbb20ac13823c4b945cedba199
SHA256:bce3ca335dc878df012c8dacb3a746a2d0f377c01b1f086ead2d665e0a3d81bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: fileUploadRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/fileUploadRenderer.directive.js
MD5: 231de69a8b11511aba2b1d554b1c237c
SHA1: 07a949eca5cea00f3244c0c327a5055e938c20f1
SHA256:09bb8467939975c92a5fed3ed5d48e62b5b4573873aa6ea55cc68f815675f4e3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: filesystemFileInputOrUpload.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/filesystemFileInputOrUpload.directive.js
MD5: f644a3106bfee156df76d5700377f70d
SHA1: c95cf943e2d57132b71a47525b512fbe46f7fed4
SHA256:2ce6c7628582dc79f62161e19e2733b679647ff423e8d8ee83474eef6ce9624d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: filesystemInputButton.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins

/config/client/js/renderer/filesystemInputButton.directive.js
MD5: dd16af124bfbff63b1bef502a1c6630d
SHA1: 26eb623f863a69f186365988808e321f1f421692
SHA256:ddf1136d4e8d24e42d48617029ea3f5bc5e80f0d75a4451fe21dfa99b9255e3b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: filesystemInputDirectory.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/filesystemInputDirectory.directive.js
MD5: 3cf7e19c8d581a144b12439098781395
SHA1: 46b927c20b57f1d0f62f3c9dff5708da55ba97c6
SHA256:1f40a5ac25e1df1292400bede1676da6016d76d0a6c761cfcfb2f67fa2257585
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: filesystemInputFile.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/filesystemInputFile.directive.js
MD5: 393bbc22a2f66c0833bf4281ed12541d
SHA1: 4a5e9d6ad48214e9ac9409f98c75c006e590ceda
SHA256:9174dd14a4fe04430ed3bd162a86d00ec8d4bafdbe4f6a3bfe54196e2b592e03
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: iconDropRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/iconDropRenderer.directive.js
MD5: d4d0176550927ff8bd5a7c26ed223c22
SHA1: 41f5aa47f2846fcc4512ffa81bc62f97d51df945
SHA256:1360c568dbbb220749a10cb45989c9f838b9defbbf43530020cbe039b77aca15
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: inlinerenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/inlinerenderer.directive.js
MD5: 4531879fc071658f5888a12116e31f0d
SHA1: 374bcc0bbcc65b4d88ff5a224731409c78a4f7b7
SHA256:032c6ac3238780e1eb1767300dae7818ccda70bb17ccb70725ea06d8ee19adf2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: keyLabelText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/keyLabelText.directive.js
MD5: 2f2a25596ec290d0f62e10a37fc973c8
SHA1: a4e327416b73eeda15ba6d1874a3bbc3849ae81e
SHA256:2a481ea7ff3b62f87adb28b57e222ef1352f1cfa73a154d63902cb0df0113b42
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: labelLink.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/labelLink.directive.js
MD5: ddc833761a08073a8a458908e5dcfa57
SHA1: 221bc834d495ab84fa96db2b84ec811ff5306680
SHA256:de1ac60b78a35c40d6680ea08cf9a0f7ec3f643e656b14a8bf24db88b532f712
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: labelText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/labelText.directive.js
MD5: 1dc9a77a6475334b814a4eb39b6e8aa0
SHA1: d0db5c5a08bd2c74dffcafcbef0ffc8438e35357
SHA256:1cb05364e04e307603df6a644178aff10fabfed16bfce4d21c86fb75f44139ba
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: licenseKeyItemRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/licenseKeyItemRenderer.directive.js
MD5: 1b7acb7f77157666bd8163e13cc47fdf
SHA1: e623aa9b016fc3d3f9fc16449dd1ac48f3e17fd3
SHA256:ac41f0893480d1086562eef9c8269ea35f4605b80fd3f60628e4a9f3d6aa73a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: licenseKeyRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/licenseKeyRenderer.directive.js
MD5: 6d48b1b05a2bd2ef4384bb996789ddca

SHA1: d1131bfe50939a01e50982034b1b7574822215bf
SHA256:8c881d970f4c71dc3a5eddb6a2028729ce9efc82dc629880885a4bd043db53ba
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: listItemRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/listItemRenderer.directive.js
MD5: edd4cd7e1b5eaf3ac7016241fffac9f1
SHA1: 17781e1ede1a58095efee23f06e3517db1196e49
SHA256:863b67000b698b39f9a643e18c7904da83b76c50a7d563347a01891a7d80bd6a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: logopreview.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/logopreview.directive.js
MD5: 84cbbf2c3c0b52d6c249e076fe48cb8f
SHA1: c63e504fabdb02f4cbe1dd2dfa110288472a4e0c
SHA256:e1b11195c665b08ffc7c19b22e7d7d77e49ed86877cd65e6bc9a166566aa5d31
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: multiLineCode.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/multiLineCode.directive.js
MD5: e2a752736b313cd15c5067b9e2f7abc6
SHA1: 2c22df117b9f45a082498e2696385eca5919534d
SHA256:c1d8916f36bc63228d52ff52432d599f6001077d784d2bf47870569daf2a99c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: multiLineText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/multiLineText.directive.js
MD5: 9769483af9509271e1ffd9602c681481
SHA1: fbb61268f1e63f705fb6d167bdb9f5138d622a18
SHA256:36e44de5802b59df141325897a839a73be22d803df0300985e3eb23ef0f060d4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: multiLingualTextRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/multiLingualTextRenderer.directive.js
MD5: c417f8278dcca4343be0b1c60d6c5fe1
SHA1: 3eda017cc7075b934736e1daf71b0d59aa412203
SHA256:c497b95a7eb0af1ef36a9733a5e9675a5ac62c094a738288ed8c021b7cd9a429
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: passwordText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/passwordText.directive.js
MD5: a762f68eb820d383f03214a0c401d090
SHA1: 05c793442f5193f2ffa3b952cd62af88309e68f6
SHA256:fba766ee79b545a364e9b8d53a5fd0df688657a201bdd25c7c6bcf3a92678337
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: reloadCategoryTrigger.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/reloadCategoryTrigger.directive.js
MD5: 231b1dc0c3b75ced21c22938f2112f28
SHA1: 468b14bd607e1485713229284a9654314a8ea7cd
SHA256:d928f424965cbc2ea8e34bd29e3b502324abb3b4781e0a7b18571ab9ebd1ddce
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: reloadSelectInputsTrigger.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/reloadSelectInputsTrigger.directive.js
MD5: ee0760c34d35b7ab1f556b36ef72504b
SHA1: cfcab22873b681c7d9019378b4c7fa9c6af49b47
SHA256:40e2a2f7b5e647a301971e061dbd5a7d614458f9172510d8f64f1b21b2347e3f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: renderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/renderer.directive.js
MD5: e6700ce9f732a1f1b614ffdcd2c94933

SHA1: 1c5c4b48b29a6b9fd8b9f560207df52cf3ff430d
SHA256:3c26aeb2ecfd733d17ff0facd86c8328a20759a6fe1b4059bbcc8221461d3574
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: repoDbRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/repoDbRenderer.directive.js
MD5: 5ef1c770c4e5fe42e93f01f633f453d3
SHA1: 5da8e6fda8968333e5a0badb6aa45020a83b6b69
SHA256:c763e8eefee951c377e2c0c54a8d52618e50224dbb458529d750701c7a1f9e96
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: repoFsRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/repoFsRenderer.directive.js
MD5: 6bf0ab3a102f1607ad605c4820851ff4
SHA1: ec76ee20ea8fc5950c233ebb71a89367fb0b5d48
SHA256:71fb520ea8562e3a06f3eabc3117b85a874092205bc7052a856faaec867e7df6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: repositoryItemRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/repositoryItemRenderer.directive.js
MD5: 35b661e3e8a0b9517b5ef113729adebf
SHA1: 451b13b299f3189adeb149487bd614b2de8ec78c
SHA256:f155af09a82a7d6babc233a77ffa620935e78b1bb8e8636ec2987241a0fec48b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: repositoryRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/repositoryRenderer.directive.js
MD5: cca1b6d749a3ff9bb3ed1e546c1ddd3f
SHA1: 295dbe208d68b96973cfde80dc8f657cdaedb7f2
SHA256:597b792888878b76bd3e67b99651b5d52c1332790765d4a6e11a9f9d3d289490
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: selectEditText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/selectEditText.directive.js
MD5: 138c6a393ed7a6530e11c3044769dfcf
SHA1: e0de09f04f68220d0a63c2bf176ccc2116654649
SHA256:acb8597cfdc18b01850bae68d8e8975015a685ba83efc92418bc49fa2bd82c4a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: selectFilteredText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/selectFilteredText.directive.js
MD5: 66bfc1fea09570aea4f49ca2ffbd4402
SHA1: c6a8af52072afed812d736557946cda5bb89885d
SHA256:3b6e11c3459f62d6f3b2fde9d97fd3b4b8368eadfb8f64202c15aa281a1b7146
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: selectLanguageChooserRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/selectLanguageChooserRenderer.directive.js
MD5: bc16961ed0ab7d39ec9aff018531127d
SHA1: 35dc075ec9e8bf818edc799c08fe24815b496c21
SHA256:270948a6daec8fb8b86232e69450d18ce8603bcf662d631c2d380654ec1d3e0d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: selectSimpleText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/selectSimpleText.directive.js
MD5: 7f8e2e88f5ba463d9a7890a9ff2bd598
SHA1: a174f4cb3f102aee45e63441a20547acec931855
SHA256:8a2fadf95686d7827db8868ee5c5d828ca31e74fc3be8dd8d3571945467d9375
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: simpleDate.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/simpleDate.directive.js
MD5: 7859e473016ba4b6c663b2de73e886d0

SHA1: 2c6104c939065689031febe53b2c4690eb17af15
SHA256:cf6b91be17479f785ea267d269c6a254a9fd14d70df735721d723e556bf07f28
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: simpleSlider.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/simpleSlider.directive.js
MD5: 00171fe096529318005c987067f6cae4
SHA1: 586d31e6a344760d84d76e12763b6f47e69618d0
SHA256:db8ceb31a065dc67a9b7d9bc2144e6906a6f0dadd1e698f77b41cc6232246aec
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: simpleText.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/simpleText.directive.js
MD5: 8c4598540efc682f3551a75bde20dfd9
SHA1: 42c3a77e9067c8d053e4dac23de2a40a70d67ec4
SHA256:b18a8129f293a7ce070aa7b9bd5edbe9eceebe36b10e82a9e6a3469c1484f3d0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: tableRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/tableRenderer.directive.js
MD5: 9c912ea0c0e6a7cd18a45ab3aa2234d2
SHA1: cb8d0ba6ae90abff58f47ae07d63f3e57dfc0723
SHA256:967fadfacccbc663230a6fc2c0242cba122ea115816585f28e1c43518005c99d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: treeRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/treeRenderer.directive.js
MD5: 0a727a5f05e3fd245c2160b5366328f1
SHA1: 678f64bfd07d434e17c8ec082ae6b65c34e80953
SHA256:926c541bf1a1faa35175ff6d0aec1875cef3da5828a2a7cd24816b3052023d10
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

configuration.zip: configuration.jar: usersandgroupsselect.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/configuration.zip/configuration.jar/com/inet/report/plugins/config/client/js/renderer/usersandgroupsselect.directive.js
MD5: 27bf7f8502a7aa8612104bf9da20aa9d
SHA1: a75f988f7790d6be413c8f962c051a78880d96d7
SHA256:c7b08fadcb0c0d0907adf944c05e79a20d065d9faebfe4472b570f5f73a976d1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.calls.zip: bc-fips.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/bc-fips.jar
MD5: fcd318de6b3707f37ef0f4f2c5195737
SHA1: 8cc7775e117fa5affb2f4bf8860fcef154a0def1
SHA256:f55fc476ede820d5c03fe87e6ced5bb0095e1dc30b387445846a3ff0274f8c0e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bc-fips	High
Vendor	jar	package name	bouncycastle	Highest
Vendor	jar	package name	bouncycastle	Low
Vendor	jar	package name	fips	Highest
Vendor	jar	package name	org	Highest
Vendor	jar	package name	provider	Highest
Vendor	Manifest	application-library-allowable-	*	Low

		codebase		
Vendor	Manifest	application-name	Bouncy Castle FIPS Provider	Medium
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Vendor	Manifest	bundle-symbolicname	bcfips	Medium
Vendor	Manifest	caller-allowable-codebase	*	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	extension-name	org.bouncycastle.bcfips	Medium
Vendor	Manifest	Implementation-Vendor	BouncyCastle.org	High
Vendor	Manifest	Implementation-Vendor-Id	org.bouncycastle	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	BouncyCastle.org	Low
Vendor	Manifest	trusted-library	true	Low
Product	file	name	bc-fips	High
Product	jar	package name	bouncycastle	Highest
Product	jar	package name	fips	Highest
Product	jar	package name	org	Highest
Product	jar	package name	permissions	Highest
Product	jar	package name	provider	Highest
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	application-name	Bouncy Castle FIPS Provider	Medium
Product	Manifest	Bundle-Name	bcfips	Medium
Product	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Product	Manifest	bundle-symbolicname	bcfips	Medium
Product	Manifest	caller-allowable-codebase	*	Low
Product	Manifest	codebase	*	Low
Product	Manifest	extension-name	org.bouncycastle.bcfips	Medium
Product	Manifest	multi-release	true	Low

Product	Manifest	permissions	all-permissions	Low
Product	Manifest	trusted-library	true	Low
Version	jar	package name	permissions	Highest
Version	Manifest	Bundle-Version	2.1.3	High
Version	Manifest	Implementation-Version	2.1.3	High

Related Dependencies

- mail.zip: bc-fips.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/bc-fips.jar
  - MD5: fcd318de6b3707f37ef0f4f2c5195737
  - SHA1: 8cc7775e117fa5affb2f4bf8860fcef154a0def1
  - SHA256: f55fc476ede820d5c03fe87e6ced5bb0095e1dc30b387445846a3ff0274f8c0e
- webserver.zip: bc-fips.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/bc-fips.jar
  - MD5: fcd318de6b3707f37ef0f4f2c5195737
  - SHA1: 8cc7775e117fa5affb2f4bf8860fcef154a0def1
  - SHA256: f55fc476ede820d5c03fe87e6ced5bb0095e1dc30b387445846a3ff0274f8c0e

Identifiers

- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress

cowork.calls.zip: bcpkix-fips.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/bcpkix-fips.jar
MD5: 22411a1dde3c6bf7de5efc2f0d428087
SHA1: 9617cb32c55d8abba1929f5a228a63686106a388
SHA256:48f418d70c9551ac9225f333e5e9dfe872b4501cc566728b6d2bc7364a2223d4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bcpkix-fips	High
Vendor	jar	package name	bouncycastle	Highest
Vendor	jar	package name	bouncycastle	Low

Vendor	jar	package name	pkix	Highest
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	application-name	Bouncy Castle FIPS PKIX API	Medium
Vendor	Manifest	automatic-module-name	org.bouncycastle.fips.pkix	Medium
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Vendor	Manifest	bundle-symbolicname	bcpkix	Medium
Vendor	Manifest	caller-allowable-codebase	*	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	extension-name	org.bouncycastle.bcfips.pkix	Medium
Vendor	Manifest	Implementation-Vendor	BouncyCastle.org	High
Vendor	Manifest	Implementation-Vendor-Id	org.bouncycastle	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	BouncyCastle.org	Low
Vendor	Manifest	trusted-library	true	Low
Product	file	name	bcpkix-fips	High
Product	jar	package name	bouncycastle	Highest
Product	jar	package name	pkix	Highest
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	application-name	Bouncy Castle FIPS PKIX API	Medium
Product	Manifest	automatic-module-name	org.bouncycastle.fips.pkix	Medium
Product	Manifest	Bundle-Name	bcpkix	Medium
Product	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Product	Manifest	bundle-symbolicname	bcpkix	Medium
Product	Manifest	caller-allowable-codebase	*	Low

Product	Manifest	codebase	*	Low
Product	Manifest	extension-name	org.bouncycastle.bcfips.pkix	Medium
Product	Manifest	multi-release	true	Low
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	trusted-library	true	Low
Version	Manifest	Bundle-Version	2.1.12	High
Version	Manifest	Implementation-Version	2.1.12	High

Related Dependencies

- mail.zip: bcpkix-fips.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/bcpkix-fips.jar
  - MD5: 22411a1dde3c6bf7de5efc2f0d428087
  - SHA1: 9617cb32c55d8abba1929f5a228a63686106a388
  - SHA256: 48f418d70c9551ac9225f333e5e9dfe872b4501cc566728b6d2bc7364a2223d4
- webserver.zip: bcpkix-fips.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/bcpkix-fips.jar
  - MD5: 22411a1dde3c6bf7de5efc2f0d428087
  - SHA1: 9617cb32c55d8abba1929f5a228a63686106a388
  - SHA256: 48f418d70c9551ac9225f333e5e9dfe872b4501cc566728b6d2bc7364a2223d4

Identifiers

- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.12:*:*:*:*:*:*:* (*Confidence*: Highest) suppress

cowork.calls.zip: bctls-fips.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/bctls-fips.jar
MD5: 8e563cfe51f203d51974a1b346e8cfdf
SHA1: 91f6d18adf4e3c81ab5487485d1a5545d991f7bd
SHA256:d2233207daecc2dfccdc317a53bd874b12c21a6dc5be78e390d8826eb726194c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bctls-fips	High

Vendor	jar	package name	bouncycastle	Highest
Vendor	jar	package name	bouncycastle	Low
Vendor	jar	package name	org	Highest
Vendor	jar	package name	tls	Highest
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	application-name	Bouncy Castle FIPS TLS API	Medium
Vendor	Manifest	automatic-module-name	org.bouncycastle.fips.tls	Medium
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Vendor	Manifest	bundle-symbolicname	bctls	Medium
Vendor	Manifest	caller-allowable-codebase	*	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	extension-name	org.bouncycastle.bcfips.tls	Medium
Vendor	Manifest	Implementation-Vendor	BouncyCastle.org	High
Vendor	Manifest	Implementation-Vendor-Id	org.bouncycastle	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	BouncyCastle.org	Low
Vendor	Manifest	trusted-library	true	Low
Product	file	name	bctls-fips	High
Product	jar	package name	bouncycastle	Highest
Product	jar	package name	org	Highest
Product	jar	package name	tls	Highest
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	application-name	Bouncy Castle FIPS TLS API	Medium
Product	Manifest	automatic-module-name	org.bouncycastle.fips.tls	Medium
Product	Manifest	Bundle-Name	bctls	Medium
Product	Manifest	bundle-requiredexecution	JavaSE-1.8	Low

Product	Manifest	bundle-symbolicname	bctls	Medium
Product	Manifest	caller-allowable-codebase	*	Low
Product	Manifest	codebase	*	Low
Product	Manifest	extension-name	org.bouncycastle.bcfips.tls	Medium
Product	Manifest	multi-release	true	Low
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	trusted-library	true	Low
Version	Manifest	Bundle-Version	2.1.24	High
Version	Manifest	Implementation-Version	2.1.24	High

Identifiers

- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.24:*:*:*:*:*:*:* (*Confidence*: Highest) suppress

cowork.calls.zip: bcutil-fips.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/bcutil-fips.jar
MD5: 8292a996f5eb514d007c7e02b8b5ebad
SHA1: c6b5c948e154766f1c4df54e0e2359537c43358a
SHA256:a30e550f06dcfa0fd7da1e9a501f111421406fa237467522b3ca05187429832d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bcutil-fips	High
Vendor	jar	package name	asn1	Low
Vendor	jar	package name	bouncycastle	Highest
Vendor	jar	package name	bouncycastle	Low
Vendor	jar	package name	its	Low
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	application-	Bouncy Castle FIPS Utility API	Medium

		name		
Vendor	Manifest	automatic-module-name	org.bouncycastle.fips.util	Medium
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Vendor	Manifest	bundle-symbolicname	bcutil	Medium
Vendor	Manifest	caller-allowable-codebase	*	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	extension-name	org.bouncycastle.bcfips.util	Medium
Vendor	Manifest	Implementation-Vendor	BouncyCastle.org	High
Vendor	Manifest	Implementation-Vendor-Id	org.bouncycastle	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	BouncyCastle.org	Low
Vendor	Manifest	trusted-library	true	Low
Product	file	name	bcutil-fips	High
Product	jar	package name	asn1	Low
Product	jar	package name	bouncycastle	Highest
Product	jar	package name	its	Low
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	application-name	Bouncy Castle FIPS Utility API	Medium
Product	Manifest	automatic-module-name	org.bouncycastle.fips.util	Medium
Product	Manifest	Bundle-Name	bcutil	Medium
Product	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Product	Manifest	bundle-symbolicname	bcutil	Medium
Product	Manifest	caller-allowable-codebase	*	Low
Product	Manifest	codebase	*	Low
Product	Manifest	extension-name	org.bouncycastle.bcfips.util	Medium
Product	Manifest	multi-release	true	Low
Product	Manifest	permissions	all-permissions	Low

Product	Manifest	trusted-library	true	Low
Version	Manifest	Bundle-Version	2.1.7	High
Version	Manifest	Implementation-Version	2.1.7	High

Related Dependencies

- mail.zip: bcutil-fips.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/bcutil-fips.jar
  - MD5: 8292a996f5eb514d007c7e02b8b5ebad
  - SHA1: c6b5c948e154766f1c4df54e0e2359537c43358a
  - SHA256: a30e550f06dcfa0fd7da1e9a501f111421406fa237467522b3ca05187429832d
- webserver.zip: bcutil-fips.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/bcutil-fips.jar
  - MD5: 8292a996f5eb514d007c7e02b8b5ebad
  - SHA1: c6b5c948e154766f1c4df54e0e2359537c43358a
  - SHA256: a30e550f06dcfa0fd7da1e9a501f111421406fa237467522b3ca05187429832d

Identifiers

- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.7:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

cowork.calls.zip: concentus.jar

Description:

This package is a pure portable Java implementation of the Opus audio compression codec (see https://opus-codec.org/ for more details). This package contains the Opus encoder, decoder, multistream codecs, and repacketizer. It does NOT contain code to parse .ogg or .opus container files or to manage RTP packet streams.

License:

LICENSE: https://raw.githubusercontent.com/lostromb/concentus/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/concentus.jar
MD5: acbe932e26d09c43a721ac8816819652
SHA1: 3658ef53df76c1fb635617c03320cd56dfdd49f3
SHA256:3584da8a1ac7e0814a03ce3c1b1e70250bf7b07668bc39eea1048796d6471ce3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	concentus	High
Vendor	jar	package name	concentus	Highest
Vendor	jar	package name	github	Highest
Vendor	jar	package name	github	Low
Vendor	jar	package name	io	Highest
Vendor	jar	package name	io	Low
Vendor	jar	package name	jaredmdobson	Highest
Vendor	jar	package name	jaredmdobson	Low
Vendor	pom	artifactid	concentus	Low
Vendor	pom	developer email	Logan.Stromberg@microsoft.com	Low
Vendor	pom	developer id	lostromb	Medium
Vendor	pom	developer name	Logan Stromberg	Medium
Vendor	pom	groupid	io.github.jaredmdobson	Highest
Vendor	pom	name	concentus	High
Vendor	pom	url	https://github.com/jaredmdobson/concentus	Highest
Product	file	name	concentus	High
Product	jar	package name	concentus	Highest
Product	jar	package name	concentus	Low
Product	jar	package name	github	Highest
Product	jar	package name	github	Low
Product	jar	package name	io	Highest
Product	jar	package name	jaredmdobson	Highest
Product	jar	package name	jaredmdobson	Low
Product	pom	artifactid	concentus	Highest
Product	pom	developer email	Logan.Stromberg@microsoft.com	Low
Product	pom	developer id	lostromb	Low
Product	pom	developer name	Logan Stromberg	Low
Product	pom	groupid	io.github.jaredmdobson	Highest
Product	pom	name	concentus	High
Product	pom	url	https://github.com/jaredmdobson/concentus	Medium
Version	pom	version	1.0.2	Highest

Identifiers

- pkg:maven/io.github.jaredmdobson/concentus@1.0.2 (*Confidence*:High)

cowork.calls.zip: config.jar

Description:

configuration library for JVM languages using HOCON files

License:

https://www.apache.org/licenses/LICENSE-2.0;description=Apache-2.0

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/config.jar
MD5: c62e4875399181f2a41573ee1fb0d000
SHA1: fc87584fea1adcf5df899e58501a470329e59b52
SHA256:47d13e3196c84f2a8ccd014ae563738c3da5b7406b38e03505ec0601a2f4fc37
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	config	High
Vendor	jar	package name	config	Highest
Vendor	jar	package name	config	Low
Vendor	jar	package name	impl	Low
Vendor	jar	package name	typesafe	Highest
Vendor	jar	package name	typesafe	Low
Vendor	Manifest	automatic-module-name	typesafe.config	Medium
Vendor	Manifest	bundle-symbolicname	com.typesafe.config	Medium
Vendor	Manifest	implementation-url	https://github.com/lightbend/config	Low
Vendor	Manifest	Implementation-Vendor	com.typesafe	High
Vendor	Manifest	Implementation-Vendor-Id	com.typesafe	Medium
Vendor	Manifest	specification-vendor	com.typesafe	Low
Product	file	name	config	High
Product	jar	package name	config	Highest
Product	jar	package name	config	Low
Product	jar	package name	impl	Low

Product	jar	package name	typesafe	Highest
Product	Manifest	automatic-module-name	typesafe.config	Medium
Product	Manifest	Bundle-Name	config	Medium
Product	Manifest	bundle-symbolicname	com.typesafe.config	Medium
Product	Manifest	Implementation-Title	config	High
Product	Manifest	implementation-url	https://github.com/lightbend/config	Low
Product	Manifest	specification-title	config	Medium
Version	jar	package name	config	Highest
Version	Manifest	Bundle-Version	1.4.9	High
Version	Manifest	Implementation-Version	1.4.9	High

Identifiers

- **None**

cowork.calls.zip: cowork.calls.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/cowork.calls.jar
MD5: 032c78759f66a93288d1eaa4d3125a18
SHA1: 158aaf2ec9fb18511e218fa1074e478b1c1dcf8d
SHA256:2df59d5f0426b09f919b935d7872382b7944951ee596d72ca1c56dbf857b7865
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	cowork.calls	High
Vendor	jar	package name	calls	Low
Vendor	jar	package name	cowork	Low
Vendor	jar	package name	inet	Low
Vendor	Manifest	built-date	2026-09-28 18:06	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High

Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	cowork.calls	High
Product	jar	package name	calls	Highest
Product	jar	package name	calls	Low
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	server	Low
Product	Manifest	built-date	2026-09-28 18:06	Low
Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	cowork.calls	High
Product	Manifest	specification-title	cowork.calls	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

cowork.calls.zip: cowork.calls.jar: calltest.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/cowork.calls.jar/com/inet/cowork/calls/js/calltest.js
MD5: edb1da0c956e07c0835e02bfc2b27f2c
SHA1: 45c1e954f399d17a16efd480c81acf886443429c
SHA256:190fd12b50417ea485b7441455da12d275edb0f93ed565a3fb970941f44a2a08
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.calls.zip: cowork.calls.jar: coworkcallsactions.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/cowork.calls.jar/com/inet/cowork/calls/js/coworkcallsactions.js
MD5: 677618c2ddb70cb833afa4f48057a58b
SHA1: 7f10f9794a318192c66ce7ebe83a539688fafa1b
SHA256:6c8e2fd67ed8662248f7339067227ee057d4f99800dfac7b0a483738010af3af
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.calls.zip: cowork.calls.jar: coworkcallsettings.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/cowork.calls.jar/com/inet/cowork/calls/js/coworkcallsettings.js
MD5: a743969fc09f26ac14e994627d7a49b1
SHA1: 53aae8c2cc018a5b65c8436448dc3192b4970fdc
SHA256:a583e3a2eaad991b2191821350516fe197df50c8b44f342c566dfdc815c67204
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.calls.zip: cowork.calls.jar: coworkcallsfactory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/cowork.calls.jar/com/inet/cowork/calls/js/coworkcallsfactory.js
MD5: 1cac1aacf948e9038d9aded963da5e07
SHA1: 3d2d77a620a3b7c4adf7031a7c0b5835f5af50dd
SHA256:dd1ee453977076db1c22a8f001f18e2afc35cad9ddc9ec409d440a4ae2321095
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.calls.zip: ice4j.jar

Description:

A Java implementation of the ICE protocol

License:

Apache-2.0: https://github.com/jitsi/ice4j/blob/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/ice4j.jar
MD5: eaffb973edafb449ec4e38955f96e267
SHA1: da8ec9b9f069da054184c90129c9cdc9078fc7e9
SHA256:dfce847c62008f044edf0f1448bf9c16b5e80de17a0994289a7581e602075532
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	ice4j	High
Vendor	jar	package name	ice	Highest
Vendor	jar	package name	ice4j	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/ice4j	Low

Vendor	Manifest	bundle-symbolicname	org.jitsi.ice4j	Medium
Vendor	pom	artifactid	ice4j	Low
Vendor	pom	developer email	dev@jitsi.org	Low
Vendor	pom	developer id	org.jitsi	Medium
Vendor	pom	developer name	Jitsi Team	Medium
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	ice4j	High
Vendor	pom	organization name	jitsi.org	High
Vendor	pom	organization url	https://jitsi.org	Medium
Vendor	pom	url	jitsi/ice4j	Highest
Product	file	name	ice4j	High
Product	jar	package name	ice	Highest
Product	jar	package name	ice4j	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/ice4j	Low
Product	Manifest	Bundle-Name	ice4j	Medium
Product	Manifest	bundle-symbolicname	org.jitsi.ice4j	Medium
Product	pom	artifactid	ice4j	Highest
Product	pom	developer email	dev@jitsi.org	Low
Product	pom	developer id	org.jitsi	Low
Product	pom	developer name	Jitsi Team	Low
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	ice4j	High
Product	pom	organization name	jitsi.org	Low
Product	pom	organization url	https://jitsi.org	Low
Product	pom	url	jitsi/ice4j	High
Version	pom	version	3.2-15-g6da2b08	Highest

Identifiers

- pkg:maven/org.jitsi/ice4j@3.2-15-g6da2b08 (*Confidence*:High)
- cpe:2.3:a:jitsi:jitsi:3.2.15.g6.da2:b08:*:*:*:*:*:* (*Confidence*:Highest) suppress

cowork.calls.zip: jicoco-config.jar

Description:

Jitsi Common Components (Configuration Utilities)

License:

"Apache-2.0";link="https://github.com/jitsi/jicoco/blob/master/LICENSE"

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jicoco-config.jar
MD5: 2b360a86dbf02f02173b1e4230e19000
SHA1: 0d026d8cf9582bc707641f68ff979da2f60876d6
SHA256:40295937ec9471edf7bb8d0602b5363c709638033a01505ead4fa99f27b52550
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jicoco-config	High
Vendor	jar	package name	config	Highest
Vendor	jar	package name	jitsi	Highest
Vendor	Manifest	build-jdk-spec	17	Low
Vendor	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/jicoco/jicoco-config	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.config	Medium
Vendor	pom	artifactid	jicoco-config	Low
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	jicoco-config	High
Vendor	pom	parent-artifactid	jicoco-parent	Low
Product	file	name	jicoco-config	High
Product	jar	package name	config	Highest
Product	jar	package name	jitsi	Highest
Product	Manifest	build-jdk-spec	17	Low
Product	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/jicoco/jicoco-config	Low
Product	Manifest	Bundle-Name	jicoco-config	Medium

Product	Manifest	bundle-symbolicname	org.jitsi.config	Medium
Product	pom	artifactid	jicoco-config	Highest
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	jicoco-config	High
Product	pom	parent-artifactid	jicoco-parent	Medium
Version	pom	version	1.1-178-ga09ed33	Highest

Identifiers

- pkg:maven/org.jitsi/jicoco-config@1.1-178-ga09ed33 (*Confidence*:High)
- cpe:2.3:a:jitsi:jitsi:1.1.178.ga09.ed33:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

cowork.calls.zip: jitsi-metaconfig.jar

Description:

jitsi-metaconfig helps solve the problems around the evolution of configuration properties

License:

Apache-2.0: https://github.com/jitsi/jitsi-metaconfig/blob/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-metaconfig.jar
MD5: f41bbbdb0704a947379e648f92de3b6a
SHA1: 2c324f329f52cf28c14236efe18427e0ce7cf411
SHA256:a5f297490bc6797376e7b814e5c23cd548af5a6d5441bce272f0f1abb07abfe2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jitsi-metaconfig	High
Vendor	jar	package name	jitsi	Highest
Vendor	jar	package name	metaconfig	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-metaconfig	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.metaconfig	Medium
Vendor	pom	artifactid	jitsi-metaconfig	Low

Vendor	pom	developer email	dev@jitsi.org	Low
Vendor	pom	developer id	org.jitsi	Medium
Vendor	pom	developer name	Jitsi Team	Medium
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	jitsi-metaconfig	High
Vendor	pom	organization name	jitsi.org	High
Vendor	pom	organization url	https://jitsi.org	Medium
Vendor	pom	url	jitsi/jitsi-metaconfig	Highest
Product	file	name	jitsi-metaconfig	High
Product	jar	package name	jitsi	Highest
Product	jar	package name	metaconfig	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-metaconfig	Low
Product	Manifest	Bundle-Name	jitsi-metaconfig	Medium
Product	Manifest	bundle-symbolicname	org.jitsi.metaconfig	Medium
Product	pom	artifactid	jitsi-metaconfig	Highest
Product	pom	developer email	dev@jitsi.org	Low
Product	pom	developer id	org.jitsi	Low
Product	pom	developer name	Jitsi Team	Low
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	jitsi-metaconfig	High
Product	pom	organization name	jitsi.org	Low
Product	pom	organization url	https://jitsi.org	Low
Product	pom	url	jitsi/jitsi-metaconfig	High
Version	pom	version	1.0-17-g58971d6	Highest

Identifiers

- pkg:maven/org.jitsi/jitsi-metaconfig@1.0-17-g58971d6 (*Confidence*:High)
- cpe:2.3:a:jitsi:jitsi:1.0.17.g58971.d6:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

cowork.calls.zip: jitsi-utils.jar

Description:

A set of basic utilities used in Jitsi projects

License:

Apache-2.0: https://github.com/jitsi/jitsi-utils/blob/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-utils.jar
MD5: fa494e8f6b723155f32c3dfb490d8e6e
SHA1: 98b8409c3d8d08aad6a501a32266a669b4252b04
SHA256:aab74933cf6945b99ac3a81d3f27a8753cc3342e97fe522e0b76c18e9ef09923
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jitsi-utils	High
Vendor	jar	package name	jitsi	Highest
Vendor	jar	package name	utils	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-utils	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.utils	Medium
Vendor	pom	artifactid	jitsi-utils	Low
Vendor	pom	developer email	dev@jitsi.org	Low
Vendor	pom	developer id	org.jitsi	Medium
Vendor	pom	developer name	Jitsi Team	Medium
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	jitsi-utils	High
Vendor	pom	organization name	jitsi.org	High
Vendor	pom	organization url	https://jitsi.org	Medium
Vendor	pom	url	jitsi/jitsi-utils	Highest
Product	file	name	jitsi-utils	High
Product	jar	package name	jitsi	Highest
Product	jar	package name	utils	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-utils	Low
Product	Manifest	Bundle-Name	jitsi-utils	Medium

Product	Manifest	bundle-symbolicname	org.jitsi.utils	Medium
Product	pom	artifactid	jitsi-utils	Highest
Product	pom	developer email	dev@jitsi.org	Low
Product	pom	developer id	org.jitsi	Low
Product	pom	developer name	Jitsi Team	Low
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	jitsi-utils	High
Product	pom	organization name	jitsi.org	Low
Product	pom	organization url	https://jitsi.org	Low
Product	pom	url	jitsi/jitsi-utils	High
Version	pom	version	1.0-150-g4ab9a3b	Highest

Identifiers

- pkg:maven/org.jitsi/jitsi-utils@1.0-150-g4ab9a3b (*Confidence*:High)
- cpe:2.3:a:jitsi:jitsi:1.0.150.g4.ab9:a3:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:utils_project:utils:1.0.150.g4.ab9:a3:*:*:*:*:*:* (*Confidence*:Highest) suppress

cowork.calls.zip: kotlin-stdlib.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/kotlin-stdlib.jar
MD5: 99b8b084c36f4bb0ecfbfcbce05dd1c2
SHA1: 94c1451890d164aed65d43b3db0b7ecef7c183e7
SHA256:2226de463d309d4a5500a481320b3dea515a6981dcae1def531fbc158884e25f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	kotlin-stdlib	High
Vendor	jar	package name	kotlin	Low
Vendor	Manifest	Implementation-Vendor	JetBrains	High
Vendor	Manifest	kotlin-runtime-component	Main	Low
Vendor	Manifest	multi-release	true	Low

Product	file	name	kotlin-stdlib	High
Product	jar	package name	kotlin	Highest
Product	Manifest	Implementation-Title	kotlin-stdlib	High
Product	Manifest	kotlin-runtime-component	Main	Low
Product	Manifest	multi-release	true	Low
Version	Manifest	Implementation-Version	2.4.20	High

Related Dependencies

- cowork.calls.zip: kotlin-reflect.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/kotlin-reflect.jar
  - MD5: a2abf34c998aa922d1b468e8937ef9a1
  - SHA1: a550e029f875982678926dc574e7b4c15ac71d8b
  - SHA256: b4aac2a4686ffdc110602ce153e4a90ffd7f37fa86fcca9d3b3aa39c08f8c2fc

Identifiers

- cpe:2.3:a:jetbrains:kotlin:2.4.20:*:*:*:*:*:*:* (*Confidence*:High) suppress

cowork.calls.zip: vosk.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/vosk.jar
MD5: 9e9331d6399fe13d7d407895e51830c6
SHA1: bc8480ade0cef39ef51c527fc3a947b6f475c953
SHA256:b463e560f3a0be68e3c75b2aa4a457fd97bc818038ea92471580fed3b00cd296
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	vosk	High
Vendor	jar	package name	vosk	Low
Product	file	name	vosk	High

Identifiers

- **None**

cowork.calls.zip: vosk.jar: libgcc_s_seh-1.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/vosk.jar/win32-x86-64/libgcc_s_seh-1.dll
MD5: 6c39c37f05b68f7515b07ea6a803d19d
SHA1: 45420d03aaae927527fcb8ea774065c617ab5515
SHA256:201bf8a54ebb490f93ea4beb20740a483bf67036b90b5720f32d0c746a72d1e9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	libgcc_s_seh-1	High
Product	file	name	libgcc_s_seh-1	High
Version	file	name	libgcc_s_seh-1	Medium
Version	file	version	1	Medium

Identifiers

- **None**

cowork.calls.zip: vosk.jar: libstdc++-6.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/vosk.jar/win32-x86-64/libstdc++-6.dll
MD5: bdd217aa63ce123986a70570edb8909b
SHA1: bedd9a223839d07dff376e06a66550f929dcfbdc
SHA256:a1d96a848a567d7657e152cfe92e2fd62da412968cc11ec8bdb04bf20ebc5747
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	libstdc++-6	High
Product	file	name	libstdc++-6	High
Version	file	name	libstdc++-6	Medium
Version	file	version	6	Medium

Identifiers

- **None**

cowork.calls.zip: vosk.jar: libvosk.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/vosk.jar/win32-x86-64/libvosk.dll
MD5: 8778133e327b5630e5bcdbaa3107533c
SHA1: 68cef503b800ab8d5c8cefb80c59c16ca8e4ab88
SHA256:9331c2f6a32cf77141af27c9750e79532718f51bbc2e3cea3c60f14ca4251e4e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	libvosk	High
Product	file	name	libvosk	High

Identifiers

- **None**

cowork.calls.zip: vosk.jar: libwinpthread-1.dll

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/vosk.jar/win32-x86-64/libwinpthread-1.dll
MD5: ecd7c5d4c6c8d905f3eed86313cf06d8
SHA1: 5b9ba8115007242535a35f29b897a6c0077b0bcb
SHA256:92caeb8a4ea281c674003462a233f3b445b685b0a6f93eb11254feda2dda9cde
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	libwinpthread-1	High
Product	file	name	libwinpthread-1	High
Version	file	name	libwinpthread-1	Medium

Version	file	version	1	Medium

Identifiers

- **None**

cowork.klipy.zip: cowork.klipy.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.klipy.zip/cowork.klipy.jar
MD5: 7ded3f3bec300cfca3d9dd9d4c31f1de
SHA1: 51585c15fa91c1b804ab7029e0880f5328e9fb2c
SHA256:26ef611b4debe9af556b40b2468a6f5224c9a0d62d78a3ab89c7ce84d4db995e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	cowork.klipy	High
Vendor	jar	package name	cowork	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	klipy	Low
Vendor	Manifest	built-date	2026-09-28 18:06	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	cowork.klipy	High
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	klipy	Highest
Product	jar	package name	klipy	Low
Product	jar	package name	server	Low
Product	Manifest	built-date	2026-09-28 18:06	Low

Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	cowork.klipy	High
Product	Manifest	specification-title	cowork.klipy	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

cowork.klipy.zip: cowork.klipy.jar: coworkklipy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.klipy.zip/cowork.klipy.jar/com/inet/cowork/klipy/js/coworkklipy.js
MD5: 0f3cec5af51780baef20686b2757d7a6
SHA1: 8bf63d0313043b114afdbd4136caef2a48b389f7
SHA256:ca35e0a3754fbc422703728eb0eb457922d0b5829a61cbe1dd4295a513217da0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.klipy.zip: cowork.klipy.jar: klipygifselector.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.klipy.zip/cowork.klipy.jar/com/inet/cowork/klipy/js/klipygifselector.directive.js
MD5: 6a07ab99d390e9b44b728863a00259c6
SHA1: 7e6c943353300b00d3ec7e15c3e512b951fa5cbe
SHA256:549b4a8267ac9ee1e1e8fe74ea6eed8574ad4c9c5cb981a55000dd4e29ef3106
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.meetingrooms.zip: cowork.meetingrooms.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.meetingrooms.zip/cowork.meetingrooms.jar
MD5: 7638061800b2c595865db795a24c6432
SHA1: 674830681b8060f0108e3d244259ef018bf17f19
SHA256:d1af0bc8eeb3ba0e5a1dfc2848b408e862813fa97cedd05089b654e43bfa9389
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	cowork.meetingrooms	High
Vendor	jar	package name	cowork	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	meetingrooms	Low
Vendor	Manifest	built-date	2026-09-28 18:06	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	cowork.meetingrooms	High
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	meetingrooms	Highest
Product	jar	package name	meetingrooms	Low
Product	jar	package name	server	Low

Product	Manifest	built-date	2026-09-28 18:06	Low
Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	cowork.meetingrooms	High
Product	Manifest	specification-title	cowork.meetingrooms	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

cowork.meetingrooms.zip: cowork.meetingrooms.jar: coworkmeetingroom.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.meetingrooms.zip/cowork.meetingrooms.jar/com/inet/cowork/meetingrooms/js/coworkmeetingroom.js
MD5: d8d75a82676baadffbcfb4fbca9cba64
SHA1: 40559ccdee37d2c24465a4e5991ed3523a667b06
SHA256:8f777d5bc8e08b5f4569aee36308879c909809cd95df590bb5f4f14f7fa05810
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.meetingrooms.zip: cowork.meetingrooms.jar: coworkmeetingroommoderator.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.meetingrooms.zip/cowork.meetingrooms.jar/com/inet/cowork/meetingrooms/js/coworkmeetingroommoderator.js
MD5: 1d74c213bd09d16bbee6cbf1f24dac24
SHA1: 65b4fb0e426aac94e16b3b50b388bcc1e135b42f

SHA256:04526775f95c3c0f9502e2fb0e15cbdad9ffc4eacb86bb306ab7843d3b11dab2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.meetingrooms.zip: cowork.meetingrooms.jar: endofmeeting.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.meetingrooms.zip/cowork.meetingrooms.jar/com/inet/cowork/meetingrooms/js/endofmeeting.js
MD5: 0281ea6e71a959ed149d54fad9386462
SHA1: f305ac2dc2ae559f53d00345fce6ee6bbae5f13c
SHA256:4470698bfb5d861a24d4c27ad1b2ebfc7b5dd2b24e700fef1e992368618bb9f2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.meetingrooms.zip: cowork.meetingrooms.jar: joinmeeting.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.meetingrooms.zip/cowork.meetingrooms.jar/com/inet/cowork/meetingrooms/js/joinmeeting.js
MD5: 398c8fe5b911dcf780426d09c7531d67
SHA1: cd6587dbc2d8eb175b72f80d95a58ccb89e3cd49
SHA256:9f04c67d31561578bd2181776f53516634da1deeda66768ead65b1f9f4233508
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.meetingrooms.zip: cowork.meetingrooms.jar: meetingrooms.maintenance.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.meetingrooms.zip/cowork.meetingrooms.jar/com/inet/cowork/meetingrooms/maintenance/meetingrooms.maintenance.js
MD5: aaf63a1e68374c34cbbca13997512af5
SHA1: 9a906438d110c13ba12870967ffdf897b07ac64f
SHA256:a74e1d547327866baf8c79ca707c7c0a9263db8ff25b7fcc36feee4cb010ccfb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.tenor.zip: cowork.tenor.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.tenor.zip/cowork.tenor.jar
MD5: 3d4f23123f128284d4fb9dbbe5942f9d
SHA1: 52354fb6db890e2c4d3413bf7f4e177786957138
SHA256:335c0369098bfaf5d7b396f41b64d77190f8f2f1741667026f4eb887c9004f15
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	cowork.tenor	High
Vendor	jar	package name	cowork	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	tenor	Low

Vendor	Manifest	built-date	2026-09-28 18:06	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	cowork.tenor	High
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	server	Low
Product	jar	package name	tenor	Highest
Product	jar	package name	tenor	Low
Product	Manifest	built-date	2026-09-28 18:06	Low
Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	cowork.tenor	High
Product	Manifest	specification-title	cowork.tenor	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

cowork.tenor.zip: cowork.tenor.jar: coworktenor.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.tenor.zip/cowork.tenor.jar/com/inet/cowork/tenor/js/coworktenor.js
MD5: 074ded7c1c1f959db8cbaa36a7ddac77
SHA1: 157a1b841e1479dfbd90ae8903538f0963320a2f
SHA256:1fbfa51d71ee0b28262612b619d499f25e49fb78ba133ac5c9203a4ef848f14c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.tenor.zip: cowork.tenor.jar: tenorgifselector.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.tenor.zip/cowork.tenor.jar/com/inet/cowork/tenor/js/tenorgifselector.directive.js
MD5: 516f4268d2b660004c9cd400beb66d61
SHA1: e60545d319c770992cf788ff856fcd9fdfba364c
SHA256:e72fa0250bd48e53549c70ade85cde898e4be7e506f23acce9b2561e5cc033a1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.waitingqueue.zip: cowork.waitingqueue.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.waitingqueue.zip/cowork.waitingqueue.jar
MD5: 172acea82f56445551516d02a53a539b
SHA1: 3a99c07a2494fe080323fee658a0b485edc60b33
SHA256:3714b839555ea03c79d4ebd70ed149868d941f6a95aaaf646a24785ae284b638
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	cowork.waitingqueue	High
Vendor	jar	package name	cowork	Low
Vendor	jar	package name	inet	Low

Vendor	jar	package name	waitingqueue	Low
Vendor	Manifest	built-date	2026-09-28 18:06	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	cowork.waitingqueue	High
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	server	Low
Product	jar	package name	waitingqueue	Highest
Product	jar	package name	waitingqueue	Low
Product	Manifest	built-date	2026-09-28 18:06	Low
Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	cowork.waitingqueue	High
Product	Manifest	specification-title	cowork.waitingqueue	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

cowork.waitingqueue.zip: cowork.waitingqueue.jar: coworkwaitingqueue.dialog.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.waitingqueue.zip/cowork.waitingqueue.jar/com/inet/cowork/waitingqueue/client/js/coworkwaitingqueue.dialog.js
MD5: 555717b4737747d476ab4d3fb8b44777
SHA1: 0d8ada1cdedf3a09256d41e34c32d02aefaead11
SHA256:4307df33a30130a3baa09a753d96e4ff85d8aee2d57fe6a55ab478be5114b1fd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.waitingqueue.zip: cowork.waitingqueue.jar: coworkwaitingqueue.indicator.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.waitingqueue.zip/cowork.waitingqueue.jar/com/inet/cowork/waitingqueue/client/js/coworkwaitingqueue.indicator.js
MD5: f4da33e42876ea622579e6ece21909e6
SHA1: 2d459499d1daa92f09a8ccf6ecec27365ad9bdda
SHA256:e3adca167fc8e5a50a692f0e603f6df210d1c10ad88e7114054f0c861960f68c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.waitingqueue.zip: cowork.waitingqueue.jar: coworkwaitingqueue.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.waitingqueue.zip/cowork.waitingqueue.jar/com/inet/cowork/waitingqueue/client/js/coworkwaitingqueue.js
MD5: a2f4e13ac1e973acc97a2e74c64142a2
SHA1: 024d38e8ba4ff1d7e481fcf28436c63f83001527
SHA256:4c4712c1d7af1cc82ca8de749b681c5a8dd03a8bd0455bab61eb4f489091504d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar
MD5: 06cb1b6d22b46500b0b891c9eb034eb1
SHA1: aa831b6f2655c91678fa7140ecd24f31973fe55c
SHA256:f92b1bd31c2830d1af2edc27b8f46b8438e77a343eb7b7c64b10176e9f2f50f5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	cowork-javadoc	High
Product	file	name	cowork-javadoc	High

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: jquery-3.7.1.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/script-files/jquery-3.7.1.min.js
MD5: 2c872dbe60f4ba70fb85356113d8b35e
SHA1: ee48592d1fff952fcf06ce0b666ed4785493afdc
SHA256:fc9a93dd241f6b045cbff0481cf4e1901becd0e12fb45166a8f17f95823f0b1a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- maintenance.zip: maintenance-javadoc.jar: jquery-3.7.1.min.js

- File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/script-files/jquery-3.7.1.min.js
- MD5: 2c872dbe60f4ba70fb85356113d8b35e
- SHA1: ee48592d1fff952fcf06ce0b666ed4785493afdc
- SHA256: fc9a93dd241f6b045cbff0481cf4e1901becd0e12fb45166a8f17f95823f0b1a

- taskplanner.zip: taskplanner-javadoc.jar: jquery-3.7.1.min.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/script-files/jquery-3.7.1.min.js
  - MD5: 2c872dbe60f4ba70fb85356113d8b35e
  - SHA1: ee48592d1fff952fcf06ce0b666ed4785493afdc
  - SHA256: fc9a93dd241f6b045cbff0481cf4e1901becd0e12fb45166a8f17f95823f0b1a

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: jquery-ui.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/script-files/jquery-ui.min.js
MD5: ab481ee8cd3ebac4edfcbd2cae5b0dde
SHA1: a3df331b23b1dc7d01d219cf426ff3148da3ac33
SHA256:4c0b2b6513452adf188402da32faea446b326e0a3362eda6fa8603e73594a567
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- maintenance.zip: maintenance-javadoc.jar: jquery-ui.min.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/script-files/jquery-ui.min.js
  - MD5: ab481ee8cd3ebac4edfcbd2cae5b0dde
  - SHA1: a3df331b23b1dc7d01d219cf426ff3148da3ac33
  - SHA256: 4c0b2b6513452adf188402da32faea446b326e0a3362eda6fa8603e73594a567
- taskplanner.zip: taskplanner-javadoc.jar: jquery-ui.min.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/script-files/jquery-ui.min.js
  - MD5: ab481ee8cd3ebac4edfcbd2cae5b0dde
  - SHA1: a3df331b23b1dc7d01d219cf426ff3148da3ac33
  - SHA256: 4c0b2b6513452adf188402da32faea446b326e0a3362eda6fa8603e73594a567

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: member-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/member-search-index.js
MD5: 8b37fe18c8c12db919de34be9f2bfe6d
SHA1: 27f33791b2e7c4a5fbe6cef87e88f2fb9de05afa
SHA256:150dfef2e5ba6aca4aa0b83613b63089f92dff9f2b832eff75597deb2777fdb6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: module-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/module-search-index.js
MD5: a33da0f469acbd03f77bf407bac505f5
SHA1: 1e996ce630c6e1ada3ea86d7b71dabca0180f8e8
SHA256:814a05983e3267d591c7e62b314eb8eb0504eee844c8a70d494f6edbaa0f4f18
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- maintenance.zip: maintenance-javadoc.jar: module-search-index.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/module-search-index.js
  - MD5: a33da0f469acbd03f77bf407bac505f5
  - SHA1: 1e996ce630c6e1ada3ea86d7b71dabca0180f8e8
  - SHA256: 814a05983e3267d591c7e62b314eb8eb0504eee844c8a70d494f6edbaa0f4f18
- taskplanner.zip: taskplanner-javadoc.jar: module-search-index.js

- File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/module-search-index.js
- MD5: a33da0f469acbd03f77bf407bac505f5
- SHA1: 1e996ce630c6e1ada3ea86d7b71dabca0180f8e8
- SHA256: 814a05983e3267d591c7e62b314eb8eb0504eee844c8a70d494f6edbaa0f4f18

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: package-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/package-search-index.js
MD5: 12de3e8aebc1196f883d1cd64faba5f7
SHA1: 5750d65e574ec334e90dc46ac2bab6b74c4ce270
SHA256:7addf543b7dfb5cc9f4d0e29e85090add93e754e53af87a5b18ec9afaaa8185b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: script.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/script-files/script.js
MD5: 14f041a73b41a06e14ae5119bf58a412
SHA1: 3bde180527bb365eea5f582d8fa6c08270c9b745
SHA256:795ddba417f4a106bbfae3c84cb2c61363e0ce9b29163eaefdc9c334db1f9b2d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- maintenance.zip: maintenance-javadoc.jar: script.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /maintenance.zip/maintenance-javadoc.jar/script-files/script.js
  - MD5: 14f041a73b41a06e14ae5119bf58a412
  - SHA1: 3bde180527bb365eea5f582d8fa6c08270c9b745
  - SHA256: 795ddba417f4a106bbfae3c84cb2c61363e0ce9b29163eaefdc9c334db1f9b2d
- taskplanner.zip: taskplanner-javadoc.jar: script.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /taskplanner.zip/taskplanner-javadoc.jar/script-files/script.js
  - MD5: 14f041a73b41a06e14ae5119bf58a412
  - SHA1: 3bde180527bb365eea5f582d8fa6c08270c9b745
  - SHA256: 795ddba417f4a106bbfae3c84cb2c61363e0ce9b29163eaefdc9c334db1f9b2d

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: search-page.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller /build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/script-files/search-page.js
MD5: 91487edb9c0528bb329ed378cd74987f
SHA1: 001ab7444e3ba1252d4daf7f870d51bb287cd4e7
SHA256:3bd59d168258fa81f6ffe473feec32bae0e0a5d571ecc89a1eb4fc04defed1b7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- maintenance.zip: maintenance-javadoc.jar: search-page.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /maintenance.zip/maintenance-javadoc.jar/script-files/search-page.js
  - MD5: 91487edb9c0528bb329ed378cd74987f
  - SHA1: 001ab7444e3ba1252d4daf7f870d51bb287cd4e7
  - SHA256: 3bd59d168258fa81f6ffe473feec32bae0e0a5d571ecc89a1eb4fc04defed1b7
- taskplanner.zip: taskplanner-javadoc.jar: search-page.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /taskplanner.zip/taskplanner-javadoc.jar/script-files/search-page.js
  - MD5: 91487edb9c0528bb329ed378cd74987f
  - SHA1: 001ab7444e3ba1252d4daf7f870d51bb287cd4e7
  - SHA256: 3bd59d168258fa81f6ffe473feec32bae0e0a5d571ecc89a1eb4fc04defed1b7

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: search.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/script-files/search.js
MD5: e1bbc8e050e9e3033a72b1e719fc3957
SHA1: 01e8b1cc5816ddc972f7e6e4dc28bf14a1dcc21c
SHA256:fb8492aa12ea5e8c74045f0f909c7f9afc12cb44ce165e1b18a4d0cd1c49908c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- maintenance.zip: maintenance-javadoc.jar: search.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/script-files/search.js
  - MD5: e1bbc8e050e9e3033a72b1e719fc3957
  - SHA1: 01e8b1cc5816ddc972f7e6e4dc28bf14a1dcc21c
  - SHA256: fb8492aa12ea5e8c74045f0f909c7f9afc12cb44ce165e1b18a4d0cd1c49908c
- taskplanner.zip: taskplanner-javadoc.jar: search.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/script-files/search.js
  - MD5: e1bbc8e050e9e3033a72b1e719fc3957
  - SHA1: 01e8b1cc5816ddc972f7e6e4dc28bf14a1dcc21c
  - SHA256: fb8492aa12ea5e8c74045f0f909c7f9afc12cb44ce165e1b18a4d0cd1c49908c

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: tag-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/tag-search-index.js

MD5: acda0a4d961a2dbb052cf81694d1c50b
SHA1: 4853e0d2a022b5098359e59d740952ee1e187c04
SHA256:4394bc27c97d0c9018c2fb763bfc045db14433b160e3c1fec16795d1d1967aaf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork-javadoc.jar: type-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/type-search-index.js
MD5: 1f280c06075bac7f07e1d2048cebddae
SHA1: 6288f494685a0fdcc73a70cd557ab0944615ac55
SHA256:c1a98b63b155105ebe140fff14219450a6e84669138ed26c587412d8e9dcb46a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar
MD5: 4e1edd5b02ef025fc9b12949d99f2eb2
SHA1: 9fa671813518555a4bca8489b15764ec336ab2ec
SHA256:d5444e9c5185918190ee099711febba5e63018021baae4da371955835b0b3e06
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Vendor	file	name	cowork	High
Vendor	jar	package name	cowork	Low
Vendor	jar	package name	i	Highest
Vendor	jar	package name	inet	Low
Vendor	jar	package name	server	Low
Vendor	Manifest	built-date	2026-09-28 18:06	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	cowork	High
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	server	Low
Product	Manifest	built-date	2026-09-28 18:06	Low
Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	cowork	High
Product	Manifest	specification-title	cowork	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

cowork.zip: cowork.jar: MessageCreationChart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/integration/diagnostics/MessageCreationChart.js

MD5: 1e063297be8b6b979454ed507bdf32d6
SHA1: ada8b640a37322f40199cff859db472b8134677b
SHA256:fa749899629d75709d52effbbe728823bb10dce9cdc691375ec62c1db6b03dff
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: cowork.diagnostics.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/integration/diagnostics/cowork.diagnostics.js
MD5: 42274b03d4a7548e6e377e7e5a6b3315
SHA1: 86876f0c8ca51c49aa9e224d33d4a2077495f9a5
SHA256:2c3026c9c1b3d34d561ad1081eb6c1229c66cad6444cb6491ef6d5724393da61
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkcomponents.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkcomponents.js
MD5: f2d0e3dd58660b9acd0c9717019e66b0
SHA1: bbdb291e564e949c92b1f2ea7b9082d7b935a8fe
SHA256:8a5339bbebaeabc37e94db782e049de48cafe0b8540c440acc4e553e25107f14
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkcontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkcontroller.js
MD5: 879ea63b6a22a9388c2323d80d1a5bb8
SHA1: f1bdb7a53ba5238a3567c3d249418fa193f7bbd0
SHA256:15f9a661c43a2d8934c7535c3004ea2fae24f22e93f99b36f4f02ba888b166a2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkconversation.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkconversation.js
MD5: 061e918dc29473c0783061bcbbf1fc59
SHA1: 668bf01c37f4c2511b960fa2b71c12967a38d202
SHA256:d266db789fb546ed1ddf4c4f8e02ce3297558656a7c8caf561d567bea38d5dc3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkfactory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkfactory.js
MD5: dd85850ee2e00bfe4ae69c12377b7330
SHA1: 9050d6562dad9669409db52b2f210245b555fd3a
SHA256:214e2422edf0da416bd08032321c32c26d271fd4130520fd0c2d0472e7071459
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkinputbox.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkinputbox.js
MD5: 2868d5bf9bf6451ba542d925fcaf9f2d
SHA1: 816d988839e014648c4f68ce71208b0706c3e092
SHA256:c5ccab9962dd832ceabf8aaaf447e34304fb6feac8f3be9bc58e6deae4deb39b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkmodel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkmodel.js
MD5: 372dfa23b97f34c3a51972c3f225c07f
SHA1: 97af54594566605c8e232260fb4c05184f63a0d0
SHA256:1985cc6210b256ca428e88ecbc5b47e234dc1e09d5200b5a0ec149d9f48bd973
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworksettingscontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworksettingscontroller.js
MD5: f03330b6a50eb2188e5714486cbc76d3
SHA1: 5186f8bf71b626e7d88bd818fb6a4f1765df5657
SHA256:daec405ffba8cbed86614fae4e666658bc39e58956e850f4189eb010ee9cea9b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: coworkstarredmessages.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/coworkstarredmessages.js
MD5: e4eb02dd824c328cab0fc64148bfd8e2
SHA1: e7d2fa8ad3461c33caa628479fbd3d78a1b0274e

SHA256:0791c8416f69740d5cd4e40dee05c75313648345749dc1c3e529eaed258bb6d6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: inetmarkdown.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/inetmarkdown.js
MD5: e2ffc59274042d1caa1ac43dddf8a10c
SHA1: c2bfbe449b77aab091a19e29d9d8ebd472187231
SHA256:5931729e41d3e1aa91dcfb6107388d141ea63ef2a1c22419a07c75d0fcb3ca43
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: showreactionscontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/showreactionscontroller.js
MD5: b72ebeef733ddaef5734b2426cae3787
SHA1: 0d9069c4e55362bcb3c54bb834bd622661348c0b
SHA256:e38cd47b134e24364d6462eba469e7d7cf76b3b1222bb1b11566b6b01e81c38e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

cowork.zip: cowork.jar: teamsettingscontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork.jar/com/inet/cowork/client/js/teamsettingscontroller.js
MD5: 666003d37e4cb2e2c505b45d600bb25c
SHA1: 6e3924ccd9c0474102f11614188203f3925da3a2
SHA256:ac682d9ac81c245a01b40de4fe0aab15d9b1d4d3a1f7dfbd29aeb5088952c9d2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar
MD5: faecee6b96770166ee250d89c38b6685
SHA1: a7ee666ddaf4084576c1be860696eb482622821c
SHA256:2ce093fdcae7e8b1beca6eeae78808c95424caa0b0e2b56989d828479af40a95
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	dashboard	High
Vendor	jar	package name	dashboard	Low
Vendor	jar	package name	inet	Low
Vendor	Manifest	built-date	2026-09-28 17:48	Low

Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	dashboard	High
Product	jar	package name	dashboard	Highest
Product	jar	package name	dashboard	Low
Product	Manifest	built-date	2026-09-28 17:48	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	dashboard	High
Product	Manifest	specification-title	dashboard	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

dashboard.zip: dashboard.jar: abstract-dashboard-widget.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/abstract-dashboard-widget.js
MD5: a5455b356d33a49a961baf0ad21040bf
SHA1: fa30233dd54ffa2ad1ffd2b99f3176456ec42212
SHA256:4560d3c508237ae0c324929ec55df98a431471e662ae770ab3b7fd719782da6f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-panel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard-panel.js
MD5: 9a9071aed1967cb2ec4f18f0442567c9
SHA1: 71ff27403a9cef0fdd93c3b474c1d4d76b4b8e53
SHA256:b0e9c75589f784533314a52da682969c3fd5d54e4bbd97e7eaec05beed6174de
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-settings.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard-settings.js
MD5: 127be77ed22e2fdcbc0374a708fedab5
SHA1: 0080d63795e89434e03d364d0fcbd807f1607770
SHA256:7052c2ed909376e626b2e0fdec794273abd6fc5817649280bd2481bb4fd7b475
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-toolbar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard-toolbar.js
MD5: dc0b749699e5fbd5b6b40291f709c6f1
SHA1: 0d2dff10c12631c3c5caa9cb8e9aca5fb56b0c68
SHA256:ac9e1bda42487acc45e442c9ffc5e54a33d2bb649d186c7ed523bb7771247164
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-chart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-chart.js
MD5: 30afed50ad10ab1fb98a6b3a072e2519
SHA1: 94bb511a882c9083072e0c6968cf22fb4eee4824
SHA256:9bb9ad6d0e00466a7c09bdf77d49176c91c46d793e472b44a53e1c98a8764d14
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-edit.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard-widget-edit.js
MD5: 762ea17ba9cd93be9d942d4ed8afde08

SHA1: ef2e59a0fe54b6519e0f7ad113c02b41c6d6a613
SHA256:fd348bf7ebc16acbca52e73c4028f6e3866983dfa42fbcfb460519afc95365cc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-error.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard-widget-error.js
MD5: e51dfb5b8583f1bdd6b9d60b59d396d4
SHA1: f37a3787634d66bbe8fa1abf656951b161c6b123
SHA256:efd49a397a6efde614037db282594cce4a6baa7dbebe57c3e6a3ebb53c35de12
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-image.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-image.js
MD5: 5ca316358c5582300a6deb6e31a92959
SHA1: 0855c9c7ed9e8275328b39f50efa380adfe06652
SHA256:20a68b62a8d0eb89c863d621f4689017cf7793120ebfb2edecaab1a980f280eb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-memo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-memo.js
MD5: d7f520a3a838ef492f325d179dd11986
SHA1: a5de25e1860d2862bd665dfd530798afa9dc95bf
SHA256:c9f91cfa6d87164342c88fecb5a860f87f32bb229c2c1fd0ab0e90c13c39317a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-progress.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-progress.js
MD5: 7cb8e5e959ccaeb221d9e3873a76d974
SHA1: 8ee26107984cf9e936ec35d0afe7144c3571b46a
SHA256:2e1c4f75f2fc80672db5c8a8c6a694675029b6bb5d872013a273d88eb43bfa99
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-rating.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-rating.js
MD5: 7032cad7feb64c3bdebf40aceaaa4af1
SHA1: 02661c14ea1732716b31419be1387d667896ca7d
SHA256:9b95c310ffadbab0d08bd9dfd70197793d09b14b2eb5817e0d625df17ad2cc53
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-table.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-table.js
MD5: 7e529169ec4cf6d608f6948323ae685b
SHA1: 97c8dc681a5ad1368b3977d5673d9f0aeb6c736a
SHA256:5d409c1e3e278d517db8a4701e278babb2a137e2b338d21683eba692565923d0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-trafficlight.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-trafficlight.js
MD5: 08eff1f97d3f963c89462cb6afde2754
SHA1: ad02a314f0a51859f33b32d21ac062e3161a70c2
SHA256:6132fc48f6734edc605fbf8807657b7a3b7521a769f2cd453e119306bf64ca95
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-trend.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-trend.js
MD5: d5d1c2bd30cec96db2b8bc7aba9cf880
SHA1: 59ffb97008bd121d5a792acbb3a9b8f4b4394980
SHA256:9c18ddae8a3dd0f31e1d6e7ad26f817ce9f82b7e50f0dddeb8fcc08f92dc1842
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget-value.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widgets/dashboard-widget-value.js
MD5: d631af047d716c7df9682ae620c869c5

SHA1: 5a7ace82ed4e4fd9b5269a5ad1e532b65b75c3f5
SHA256:5ae861ee8b035645ae5fa1a725e486b91c32743cfc08c6b5d88050e8927150f5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard-widget.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard-widget.js
MD5: 5b7e489537349706777f8b06e82d25f3
SHA1: 20c035e1ff4d54b7b4e277d5d11f66b71f930ece
SHA256:8626818dcb28eb532c56279c9f3223f00c213e3440b80381d4553e702a62840c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboard.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboard.js
MD5: f99614f7ef08aeca38926e873d9068ec
SHA1: 024f76da4d774d2c65e8febe703ce3f6cdad375c
SHA256:3ca27c817ce8dafca8bf3a046f05cbfe3bb7cadd919f83bbb7bcdc66147f16a0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboardcontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboardcontroller.js
MD5: 38fd4795bf0a11e9e7d90e276a6bb111
SHA1: 442a49553dff0719f9daf19c0e995dbec303d32f
SHA256:b1ca901846e8238f34b6fa13b64ae4718fb57842b27626030e41fbad650fa434
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: dashboardfactory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/dashboardfactory.js
MD5: 25d42ec0f27311b707e2a7288f9e33c3
SHA1: e873961f1bb8ef29dd776b3641d6e55b24b9b20d
SHA256:c8aa0b23ba9b1ead30e87b26537c9afdce1333f0a1bbf3d835c1c677ae15a690
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-bgimage.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-bgimage.js
MD5: 2fc3049e844e0e1be9a35798b799ffe1
SHA1: 2f64bcb3b0e2a2c5bb53ae3ff0d279e7a1761c82
SHA256:fad70f8465fa884d4f0592004d60016336a33f9a4c60cdf6efb0b6daa5ba0515
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-colorpalettechooser.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-colorpalettechooser.js
MD5: 854456f56ceef35e97c1122ec6898549
SHA1: 291cd25b59f460e7a37a03f2317d7330fd21288c
SHA256:02b714b6920b4568dda37ad1a6f679d3791622317c8d0284e3075eb9cc4cf308
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-integrations.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-integrations.js
MD5: f785b0ab1008dd593c70424c1bfc119e
SHA1: e047ed11cdc1560776b79dde2097464db5c87599
SHA256:8fbc2e99a060b9f7153e7bf96af749cacf13cf93617571b18351459c80acffd4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-permissions.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-permissions.js
MD5: 1e8560ff11c39552aa090ad2eb99dda0
SHA1: dbc32a0ed62d14ffa70657e1bb696c9c0e987955
SHA256:51652632977b0fd6c910520e90349387949f17ae107d3243f56e35c57c274ea1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-tablecolumns.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-tablecolumns.js
MD5: 0b477311d85dc85d6ebf6312a57b470f

SHA1: 4b94573b471797c3a918d6c53504fa35d2e322eb
SHA256:1b9fae1de70c73f67936fee22ddd302cd7d036786613382e6d7246b179dc4ae3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-trafficlightcolorrange.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-trafficlightcolorrange.js
MD5: 78aa96f32ebc0953384d5562b3d752d5
SHA1: f5e3e4190eff516a99f2340712e6a121824d600b
SHA256:37d814737b3e6ca4e43cd4abd631d0038e65f22e65ab79ca5e0240396c320e64
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: ui-dashboard-valuehighlights.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/uisettings/ui-dashboard-valuehighlights.js
MD5: c9012e784f678169d46b2eb3cf6ab89c
SHA1: eb9fb9cf3b01da5cb31d28f6f660261cb9f7d8c0
SHA256:1dbd3917abdae40e38fec9e6c1160db33a77882263e965baf3dd1c61169338e0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: user-selection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/user-selection.js
MD5: cd15090b453d9201236f30f1741d7851
SHA1: 5e4ec536be05c55163ea6dfa689aa84ce177dbdc
SHA256:10aaf6f2568cce36e70577c1a59b744cd51cacf158c56500958e27ec6a67e96b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: widget-chooser.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widget-chooser.js
MD5: 752b30ba37d816d92dddcf998bf8600a
SHA1: 36bffa677e937f880d94f0efddcd61172ae6a16b
SHA256:c04881ba9826562b59244fb629140d0c90c5c4c8cd2bebd283d7015ff713fe34
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: widget-paste-area.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widget-paste-area.js
MD5: 49bfb8b5101b77700043fa1e12f8a0ab
SHA1: 6da543a80e1b43b2f3b90b8d87e1b61937a1bf76
SHA256:25581f9a62666a8fd132d893c7621d02a12b9871a6f4bd77fd957622b8497236
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: widget-placeholder.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widget-placeholder.js
MD5: 26339fcdaa9b45c9766d1e7099b2668f
SHA1: c18e8b57e91c5a73fc35bccc68f54a947ba8574a
SHA256:331db9473fe3702f4cd0b8a8d29061cfd75fac7428fc0c6203a6284cd32cfe34
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

dashboard.zip: dashboard.jar: widget-settings.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/dashboard.zip/dashboard.jar/com/inet/dashboard/client/js/widget-settings.js
MD5: c7ddf107966b38cc7e620abf201e4081
SHA1: b99e782f244defbaa311779f46b855e9f556717d
SHA256:938975e13d3651b71c65ed65987c30dfe3e47264541f5bc2f342f0a682a43a2b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar
MD5: 0e6e462db802dc38809e467360782611
SHA1: 28453fa208e96c5d79f978b494301eb957fc1c47
SHA256:507b95dee317d5a78d8fd3e7ca066272ddea24e7cdf17bdf00a2c86e37243bd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	diagnostics	High
Vendor	jar	package name	diagnostics	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	shared	Low
Vendor	Manifest	built-date	2026-09-28 17:42	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium

Product	file	name	diagnostics	High
Product	jar	package name	diagnostics	Highest
Product	jar	package name	diagnostics	Low
Product	jar	package name	shared	Highest
Product	jar	package name	shared	Low
Product	jar	package name	widgets	Low
Product	Manifest	built-date	2026-09-28 17:42	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	diagnostics	High
Product	Manifest	specification-title	diagnostics	Medium
Version	jar	package name	shared	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: MemoryPieChart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/information/resources/MemoryPieChart.js
MD5: 30c425524c8a78004a3fe26b5a4a7383
SHA1: 9275a0816480a5aa09699e563277687cdf12817d
SHA256:fdf2f20ce7808cfb867c2b4c415f04c338999a58d31b463816c8096870b62e99
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: MemoryUsageChart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/information/resources/MemoryUsageChart.js
MD5: 3ff19f37cf579b966edc17fce99b8782
SHA1: a0d59a7b8066135ffeef91e8e8b5da5a6be1cbe7
SHA256:fb8641bfa995b72d6de205c294a5d54b4537e3710b6b7ff52e83eff21cac617b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: WebServerErrorChart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/webserver/resources/WebServerErrorChart.js
MD5: 862f696da56aba3a26f17749db48a68b
SHA1: f6008f6b7c5f9964953a9e83273866521b367a96
SHA256:ef43076f171fca635b94372d15aa89f22c210284cb1dd386e252f9451afc77e8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: benchmarkCtrl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/resources/benchmarkCtrl.js
MD5: 9eaeff897d71b988456b1081f7baa57e

SHA1: 8dc7208ccfa11ba9eb736aaee676e9c7f2f62146
SHA256:3457f3446ce7a565f734ecd3aa8712884c713b10dd97713ffab9cf196becafc9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: client-server.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/clientserver/client-server.js
MD5: ed99b5c44d3bc1b8ac58f9789deeeaad
SHA1: 395f6826c7341821fad523ebdca6df4ccb4fd1e2
SHA256:535726b9cd6612bfcdb50ff9a50c6b6e4eb5b74fdc4216fbb36ba25178415335
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: contact-support-files.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/support/resources/contact-support-files.js
MD5: 777189dbbd25df742097c66357ba470d
SHA1: fa66a0401c715201668e38c9daab05a2d3135336
SHA256:5ebe33742ed60e7b10d5f7ba7c7248a13fadf2b9b71d9794878331b1e4f15095
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: contact-support-loader.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/support/resources/contact-support-loader.js
MD5: 1e5ed34eb13d078469a714b2fdbbf48f
SHA1: 1a47fc1d275fbce92e33551aec254fd748805fdb
SHA256:8191eae5d96ede81613001b5b961d16a70beffa87868233945306ce2a0afaab6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: contact-support-panel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/support/resources/contact-support-panel.js
MD5: f9248f93a8b7d4b0a23e36145d33ae67
SHA1: 02c8f3bf0b9adc6270c20526bb264d9d12ca8879
SHA256:a32c873394aa4e7992f2597b7793d855299ec1cb8c6fc35126c60f6480cd41d5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: contact-support-selection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/support/resources/contact-support-selection.js
MD5: d0fd27e1f9b8f2439e51257729987317
SHA1: 107f03801c4d219958ba96a9b9dc3fe091651435
SHA256:9cf758b71baec7512e6f6caa4dc06a2ff8dabd34d0c80d4cae4b6056fc786145
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: contact-support.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/support/resources/contact-support.js
MD5: 67ddd4a2dda6e2e72f9c71345e387edd
SHA1: 543444613db44833f7ebd05241376c9aed8e5442
SHA256:5ff4cb5a03a204a75c7750d454b5717f2e7bbcb81beff6463c7408d428d874a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: contactCtrl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/support/resources/contactCtrl.js
MD5: 0cb2d1d2de639171e546068e00924eeb
SHA1: 747554431f73705e0d8e8c38dbe1d391367a02fe
SHA256:03df459a8f109080b3ef6abb334e2c8a986a8e3577f66d6e344a96e0a0ccdba9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/resources/js/controller.js
MD5: c9d9a63b248de3b1ab32753b2652581f
SHA1: 9e9f1cf1ddcea2a7ae541d2a67b0f36d68514e77
SHA256:6ab396c52d329bb05ffc977b19f70afaee28b05f93ed53e7766369f734126485
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: cpu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/cpu/cpu.js
MD5: 249d2c1b94bbcf571319a855cbc1af47

SHA1: 6bdacb59d89d9e103e8a85ccfd9239eb931d4682
SHA256:80e5a5792052c04e314d61e3f8ab581475f303d4770109c42d19d3060941a612
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: cpuspeed.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/cpuspeed/cpuspeed.js
MD5: ec93fbb827070fdee2db352c88e7b0a0
SHA1: fbbc1f162333ff280f1a24eb4de079916673b579
SHA256:c491356a04a12726d7c3083cadbed3f147ca67f567de2c2529043d466e63f3e4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: directives.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/resources/js/directives.js
MD5: c7436529172605f449dda5c983dc74dd
SHA1: e7fd8c8ccf06d2fadce799bb442b4b8bc10fcad4
SHA256:993aecee895d9e18dd484cbcfc7b1b908db6dd2fe5a8078bf664faa39070dbe7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: errorHistoryChart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/logging/resources/errorHistoryChart.js
MD5: 3dc8396c86a2fbaae0eafbf0971359e7
SHA1: be11eddc8f2b255ee2a5c5509714db7f1161aa8b
SHA256:d830b7e8dfbdc2c32b7cf377dabba62d41338b7df1de4fd696e3a76093b1a973
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: global.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/resources/js/global.js
MD5: 64802e20bf5a9a5339db077b76120804
SHA1: d213b8c04f236ee22ab04da139fb32d33743c618
SHA256:30fbbfb604a6ec9cf8dcf1e20dcebced4abe870ea419122f8c89fd5954b64f16
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: harddisk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/harddisk/harddisk.js
MD5: 538fd0fdeb11c4fa3dd2ac88c8711204
SHA1: 80957f16c25af55fc467e6c5af84153a595115c8
SHA256:a7762d8a143e8ac4eb9931e082988207cd45ab55d088120ff28d5f833fc09c2e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: heapdumpCtrl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/dump/resources/heapdumpCtrl.js
MD5: 401a3b35d15764088ac52d3768554482
SHA1: 43448c8da29151d9ce460dc48a8f181e9264087a
SHA256:f1a8c5440714bdf4d237f4aba6186656fe5e502ad2a111745e363ee7f8fc2f0e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: informationCtrl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/information/resources/informationCtrl.js
MD5: b1b97633efb6513ee5ee1bf8d1c75e62
SHA1: 5271d00c40c6144e4e03732218ff007097de9dca
SHA256:f487b2331964e1d5942cddb37b03f9bb4bc252a6c49567ef60b10845c784b1c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: intArrayUtils.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/intArrayUtils.js
MD5: 132205ce288f4d0108593ba2adf79e7f
SHA1: b1fc530ffd7332db05d9b5431535ec0beb9ff688
SHA256:089688ab933277e0148ec91a8bd6d1d3d6e1030ec0216139675a78f8c9fd672e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: iospeed.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/iospeed/iospeed.js
MD5: 41f51d9c89d83c0c9f2a318f49fe7270

SHA1: ccee214fdd13502065ec9b41a199fb1c3941475e
SHA256:d25634e9546abdaf6828d95582b58bad9cea248c0cf8d027d318f8641941e75c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: jobs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/jobs/resources/jobs.js
MD5: c86f20826acb4cd47c7bd5dbfb75b0d4
SHA1: 91bc3730aac03d2108e538843d28f0e47d531bc2
SHA256:392dd734b01789eb4d38f999bfa2cc439550d8bb4321024a2047179676315e47
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: logging.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/logging/resources/logging.js
MD5: 0576bea979f25b530bf421fff073f651
SHA1: 4423880a3160fa1cf0ad9353c3ba50abbac476e9
SHA256:44334c09db13b3d757f5c23fd8726fbaf4138939778e1c4f0fec7fb6b93465fd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: memory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/benchmark/tasks/memory/memory.js
MD5: f18834232e1c1c47fbdca4d03ad4eeb9
SHA1: 74db18f6a0b6cd0dc2e345b47dab39558bced4f8
SHA256:5c0c8e278674ba7e3e5d9f530448f98895b7c72eea9183e889f356492477bea2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: overviewCtrl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/overview/resources/overviewCtrl.js
MD5: 80f5e4358aa6a9ba6d35c364803e6c6a
SHA1: 43c0492bb6e31b22174edb46514f0981930d2e39
SHA256:cdf4ae1ac491e48bcb17849a4b9ccdfeb5eea517798c0dc10fe13fb75b1eca99
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: pde.diagnostics.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/widgets/webserver/resources/pde.diagnostics.js
MD5: b204072262f58feda2be583defe7fb22
SHA1: b7ac04cf8cddb4fe14358b1a593fda422011b643
SHA256:ec9425761f80cb65cbbf6cc53d587eea8c1afdd9e4e62a291e4e943f990ea929
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: timeformat.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/resources/js/timeformat.js
MD5: 31e9928c521c394f829c570f248fab50
SHA1: 97977864881447d98bab1568b64f96115f4a4d4a
SHA256:f96d3c13acc616439828fdcf4a368dedb6f8a740eb44cef5980b659ee9c07845
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

diagnostics.zip: diagnostics.jar: usermenu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/diagnostics.zip/diagnostics.jar/com/inet/shared/diagnostics/resources/js/usermenu.js
MD5: 194282c1d922be86f2761862f7ae054d
SHA1: 5eeac60781e651036358d5f6ad74c3f1c55d14e4
SHA256:92833bc86e6566be1649780fc5c58ad2e1e98c578efe967deb9dc2acd1052ac0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

hamcrest-3.0.jar

Description:

Core API and libraries of hamcrest matcher framework.

License:

BSD-3-Clause: https://raw.githubusercontent.com/hamcrest/JavaHamcrest/master/LICENSE

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.hamcrest/hamcrest/3.0/8fd9b78a8e6a6510a078a9e30e9e86a6035cfaf7/hamcrest-3.0.jar
MD5: 781023c38b054e9cf1c818c77895e1eb
SHA1: 8fd9b78a8e6a6510a078a9e30e9e86a6035cfaf7
SHA256:5d66b6a4a680755cb6ed7cb104fa7835ef644667586ff0737adeb977c39ecdbc
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	hamcrest	High
Vendor	gradle	artifactid	hamcrest	Highest
Vendor	gradle	groupid	org.hamcrest	Highest
Vendor	jar	package name	hamcrest	Highest
Vendor	jar	package name	hamcrest	Low
Vendor	Manifest	automatic-module-name	org.hamcrest	Medium
Vendor	Manifest	bundle-	org.hamcrest	Medium

		symbolicname		
Vendor	Manifest	Implementation-Vendor	hamcrest.org	High
Vendor	pom	artifactid	hamcrest	Low
Vendor	pom	developer id	joewalnes	Medium
Vendor	pom	developer id	npryce	Medium
Vendor	pom	developer id	sf105	Medium
Vendor	pom	developer name	Joe Walnes	Medium
Vendor	pom	developer name	Nat Pryce	Medium
Vendor	pom	developer name	Steve Freeman	Medium
Vendor	pom	groupid	org.hamcrest	Highest
Vendor	pom	name	Hamcrest	High
Vendor	pom	url	http://hamcrest.org/JavaHamcrest/	Highest
Product	file	name	hamcrest	High
Product	gradle	artifactid	hamcrest	Highest
Product	jar	package name	hamcrest	Highest
Product	Manifest	automatic-module-name	org.hamcrest	Medium
Product	Manifest	Bundle-Name	org.hamcrest	Medium
Product	Manifest	bundle-symbolicname	org.hamcrest	Medium
Product	Manifest	Implementation-Title	hamcrest	High
Product	pom	artifactid	hamcrest	Highest
Product	pom	developer id	joewalnes	Low
Product	pom	developer id	npryce	Low
Product	pom	developer id	sf105	Low
Product	pom	developer name	Joe Walnes	Low
Product	pom	developer name	Nat Pryce	Low
Product	pom	developer name	Steve Freeman	Low
Product	pom	groupid	org.hamcrest	Highest
Product	pom	name	Hamcrest	High
Product	pom	url	http://hamcrest.org/JavaHamcrest/	Medium
Version	file	version	3.0	High
Version	gradle	version	3.0	Highest
Version	Manifest	Implementation-Version	3.0	High
Version	pom	version	3.0	Highest

Identifiers

- pkg:maven/org.hamcrest/hamcrest@3.0 (*Confidence*:High)

help.zip: commons-beanutils.jar

Description:

Apache Commons BeanUtils provides an easy-to-use but flexible wrapper around reflection and introspection.

License:

https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/commons-beanutils.jar
MD5: 32ed51f196dfda19e0dc1ce53eeed29e
SHA1: ac03ea606d13de04c2e4508227680faff151f491
SHA256:9e44ba68ec9a3f21286fa2a8bbb003b735c0f69101bb43144b79f4f8aaa74709
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	commons-beanutils	High
Vendor	jar	package name	apache	Highest
Vendor	jar	package name	beanutils	Highest
Vendor	jar	package name	commons	Highest
Vendor	Manifest	build-jdk-spec	21	Low
Vendor	Manifest	bundle-docurl	https://commons.apache.org/proper/commons-beanutils	Low
Vendor	Manifest	bundle-symbolicname	org.apache.commons.commons-beanutils	Medium
Vendor	Manifest	Implementation-Vendor	The Apache Software Foundation	High
Vendor	Manifest	Implementation-Vendor-Id	org.apache	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	specification-vendor	The Apache Software Foundation	Low
Vendor	pom	artifactid	commons-beanutils	Low
Vendor	pom	developer email	britter@apache.org	Low

Vendor	pom	developer email	chtompki@apache.org	Low
Vendor	pom	developer email	craigmcc@apache.org	Low
Vendor	pom	developer email	dion@apache.org	Low
Vendor	pom	developer email	epugh@apache.org	Low
Vendor	pom	developer email	geirm@apache.org	Low
Vendor	pom	developer email	ggregory at apache.org	Low
Vendor	pom	developer email	jcarman@apache.org	Low
Vendor	pom	developer email	jconlon@apache.org	Low
Vendor	pom	developer email	jstrachan@apache.org	Low
Vendor	pom	developer email	morgand@apache.org	Low
Vendor	pom	developer email	mvdb@apache.org	Low
Vendor	pom	developer email	niallp@apache.org	Low
Vendor	pom	developer email	rdonkin@apache.org	Low
Vendor	pom	developer email	rwaldhoff@apache.org	Low
Vendor	pom	developer email	sanders@apache.org	Low
Vendor	pom	developer email	scolebourne@apache.org	Low
Vendor	pom	developer email	skitching@apache.org	Low
Vendor	pom	developer email	stain@apache.org	Low
Vendor	pom	developer email	tobrien@apache.org	Low
Vendor	pom	developer email	yoavs@apache.org	Low
Vendor	pom	developer id	britter	Medium
Vendor	pom	developer id	chtompki	Medium
Vendor	pom	developer id	craigmcc	Medium
Vendor	pom	developer id	dion	Medium
Vendor	pom	developer id	epugh	Medium
Vendor	pom	developer id	geirm	Medium
Vendor	pom	developer id	ggregory	Medium
Vendor	pom	developer id	jcarman	Medium
Vendor	pom	developer id	jconlon	Medium
Vendor	pom	developer id	jstrachan	Medium
Vendor	pom	developer id	morgand	Medium
Vendor	pom	developer id	mvdb	Medium
Vendor	pom	developer id	niallp	Medium
Vendor	pom	developer id	rdonkin	Medium
Vendor	pom	developer id	rwaldhoff	Medium

Vendor	pom	developer id	sanders	Medium
Vendor	pom	developer id	scolebourne	Medium
Vendor	pom	developer id	skitching	Medium
Vendor	pom	developer id	stain	Medium
Vendor	pom	developer id	tobrien	Medium
Vendor	pom	developer id	yoavs	Medium
Vendor	pom	developer name	Benedikt Ritter	Medium
Vendor	pom	developer name	Craig McClanahan	Medium
Vendor	pom	developer name	David Eric Pugh	Medium
Vendor	pom	developer name	Dion Gillard	Medium
Vendor	pom	developer name	Gary Gregory	Medium
Vendor	pom	developer name	Geir Magnusson Jr.	Medium
Vendor	pom	developer name	James Carman	Medium
Vendor	pom	developer name	James Strachan	Medium
Vendor	pom	developer name	John E. Conlon	Medium
Vendor	pom	developer name	Martin van den Bemt	Medium
Vendor	pom	developer name	Morgan James Delagrange	Medium
Vendor	pom	developer name	Niall Pemberton	Medium
Vendor	pom	developer name	Rob Tompkins	Medium
Vendor	pom	developer name	Robert Burrell Donkin	Medium
Vendor	pom	developer name	Rodney Waldhoff	Medium
Vendor	pom	developer name	Scott Sanders	Medium
Vendor	pom	developer name	Simon Kitching	Medium
Vendor	pom	developer name	Stephen Colebourne	Medium
Vendor	pom	developer name	Stian Soiland-Reyes	Medium
Vendor	pom	developer name	Tim O'Brien	Medium
Vendor	pom	developer name	Yoav Shapira	Medium
Vendor	pom	developer org	The Apache Software Foundation	Medium
Vendor	pom	developer org URL	https://www.apache.org/	Medium
Vendor	pom	groupid	commons-beanutils	Highest
Vendor	pom	name	Apache Commons BeanUtils	High
Vendor	pom	parent-artifactid	commons-parent	Low
Vendor	pom	parent-groupid	org.apache.commons	Medium
Vendor	pom	url	https://commons.apache.org/proper/commons-beanutils	Highest

Product	file	name	commons-beanutils	High
Product	jar	package name	apache	Highest
Product	jar	package name	beanutils	Highest
Product	jar	package name	commons	Highest
Product	Manifest	build-jdk-spec	21	Low
Product	Manifest	bundle-docurl	https://commons.apache.org/proper/commons-beanutils	Low
Product	Manifest	Bundle-Name	Apache Commons BeanUtils	Medium
Product	Manifest	bundle-symbolicname	org.apache.commons.commons-beanutils	Medium
Product	Manifest	Implementation-Title	Apache Commons BeanUtils	High
Product	Manifest	multi-release	true	Low
Product	Manifest	specification-title	Apache Commons BeanUtils	Medium
Product	pom	artifactid	commons-beanutils	Highest
Product	pom	developer email	britter@apache.org	Low
Product	pom	developer email	chtompki@apache.org	Low
Product	pom	developer email	craigmcc@apache.org	Low
Product	pom	developer email	dion@apache.org	Low
Product	pom	developer email	epugh@apache.org	Low
Product	pom	developer email	geirm@apache.org	Low
Product	pom	developer email	ggregory at apache.org	Low
Product	pom	developer email	jcarman@apache.org	Low
Product	pom	developer email	jconlon@apache.org	Low
Product	pom	developer email	jstrachan@apache.org	Low
Product	pom	developer email	morgand@apache.org	Low
Product	pom	developer email	mvdb@apache.org	Low
Product	pom	developer email	niallp@apache.org	Low
Product	pom	developer email	rdonkin@apache.org	Low
Product	pom	developer email	rwaldhoff@apache.org	Low
Product	pom	developer email	sanders@apache.org	Low
Product	pom	developer email	scolebourne@apache.org	Low
Product	pom	developer email	skitching@apache.org	Low
Product	pom	developer email	stain@apache.org	Low
Product	pom	developer email	tobrien@apache.org	Low
Product	pom	developer email	yoavs@apache.org	Low
Product	pom	developer id	britter	Low

Product	pom	developer id	chtompki	Low
Product	pom	developer id	craigmcc	Low
Product	pom	developer id	dion	Low
Product	pom	developer id	epugh	Low
Product	pom	developer id	geirm	Low
Product	pom	developer id	ggregory	Low
Product	pom	developer id	jcarman	Low
Product	pom	developer id	jconlon	Low
Product	pom	developer id	jstrachan	Low
Product	pom	developer id	morgand	Low
Product	pom	developer id	mvdb	Low
Product	pom	developer id	niallp	Low
Product	pom	developer id	rdonkin	Low
Product	pom	developer id	rwaldhoff	Low
Product	pom	developer id	sanders	Low
Product	pom	developer id	scolebourne	Low
Product	pom	developer id	skitching	Low
Product	pom	developer id	stain	Low
Product	pom	developer id	tobrien	Low
Product	pom	developer id	yoavs	Low
Product	pom	developer name	Benedikt Ritter	Low
Product	pom	developer name	Craig McClanahan	Low
Product	pom	developer name	David Eric Pugh	Low
Product	pom	developer name	Dion Gillard	Low
Product	pom	developer name	Gary Gregory	Low
Product	pom	developer name	Geir Magnusson Jr.	Low
Product	pom	developer name	James Carman	Low
Product	pom	developer name	James Strachan	Low
Product	pom	developer name	John E. Conlon	Low
Product	pom	developer name	Martin van den Bemt	Low
Product	pom	developer name	Morgan James Delagrange	Low
Product	pom	developer name	Niall Pemberton	Low
Product	pom	developer name	Rob Tompkins	Low
Product	pom	developer name	Robert Burrell Donkin	Low
Product	pom	developer name	Rodney Waldhoff	Low

Product	pom	developer name	Scott Sanders	Low
Product	pom	developer name	Simon Kitching	Low
Product	pom	developer name	Stephen Colebourne	Low
Product	pom	developer name	Stian Soiland-Reyes	Low
Product	pom	developer name	Tim O'Brien	Low
Product	pom	developer name	Yoav Shapira	Low
Product	pom	developer org	The Apache Software Foundation	Low
Product	pom	developer org URL	https://www.apache.org/	Low
Product	pom	groupid	commons-beanutils	Highest
Product	pom	name	Apache Commons BeanUtils	High
Product	pom	parent-artifactid	commons-parent	Medium
Product	pom	parent-groupid	org.apache.commons	Medium
Product	pom	url	https://commons.apache.org/proper/commons-beanutils	Medium
Version	Manifest	Bundle-Version	1.11.0	High
Version	Manifest	Implementation-Version	1.11.0	High
Version	pom	parent-version	1.11.0	Low
Version	pom	version	1.11.0	Highest

Identifiers

- pkg:maven/commons-beanutils/commons-beanutils@1.11.0 (*Confidence*:High)
- cpe:2.3:a:apache:commons_beanutils:1.11.0:*:*:*:*:*:*:* (*Confidence*:Highest)

suppress

help.zip: commons-digester3.jar

Description:

The Apache Commons Digester package lets you configure an XML to Java object mapping module which triggers certain actions called rules whenever a particular pattern of nested XML elements is recognized.

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/commons-digester3.jar

MD5: 41d2c62c7aedafa7a3627794abc83f71
SHA1: c3f68c5ff25ec5204470fd8fdf4cb8feff5e8a79
SHA256:1c150e3d2df4b4237b47e28fea2079fb0da324578d5cca6a5fed2e37a62082ec
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	commons-digester3	High
Vendor	jar	package name	apache	Highest
Vendor	jar	package name	commons	Highest
Vendor	jar	package name	digester	Highest
Vendor	jar	package name	digester3	Highest
Vendor	jar	package name	rules	Highest
Vendor	Manifest	bundle-docurl	http://commons.apache.org/digester/	Low
Vendor	Manifest	bundle-symbolicname	org.apache.commons.digester	Medium
Vendor	Manifest	implementation-build	tags/DIGESTER3_3_2_RC2@r1212807; 2011-12-10 15:57:06+0100	Low
Vendor	Manifest	Implementation-Vendor	The Apache Software Foundation	High
Vendor	Manifest	Implementation-Vendor-Id	org.apache	Medium
Vendor	Manifest	specification-vendor	The Apache Software Foundation	Low
Vendor	pom	artifactid	commons-digester3	Low
Vendor	pom	developer email	craigmcc@apache.org	Low
Vendor	pom	developer email	jfarcand@apache.org	Low
Vendor	pom	developer email	jstrachan@apache.org	Low
Vendor	pom	developer email	jvanzyl@apache.org	Low
Vendor	pom	developer email	mbenson AT apache DOT org	Low
Vendor	pom	developer email	rahul AT apache DOT org	Low
Vendor	pom	developer email	rdonkin@apache.org	Low
Vendor	pom	developer email	sanders@totalsync.com	Low
Vendor	pom	developer email	simonetripodi AT apache DOT org	Low
Vendor	pom	developer email	skitching@apache.org	Low
Vendor	pom	developer email	tobrien@apache.org	Low
Vendor	pom	developer id	craigmcc	Medium
Vendor	pom	developer id	jfarcand	Medium
Vendor	pom	developer id	jstrachan	Medium

Vendor	pom	developer id	jvanzyl	Medium
Vendor	pom	developer id	mbenson	Medium
Vendor	pom	developer id	rahul	Medium
Vendor	pom	developer id	rdonkin	Medium
Vendor	pom	developer id	sanders	Medium
Vendor	pom	developer id	simonetripodi	Medium
Vendor	pom	developer id	skitching	Medium
Vendor	pom	developer id	tobrien	Medium
Vendor	pom	developer name	Craig McClanahan	Medium
Vendor	pom	developer name	James Strachan	Medium
Vendor	pom	developer name	Jason van Zyl	Medium
Vendor	pom	developer name	Jean-Francois Arcand	Medium
Vendor	pom	developer name	Matt Benson	Medium
Vendor	pom	developer name	Rahul Akolkar	Medium
Vendor	pom	developer name	Robert Burrell Donkin	Medium
Vendor	pom	developer name	Scott Sanders	Medium
Vendor	pom	developer name	Simon Kitching	Medium
Vendor	pom	developer name	Simone Tripodi	Medium
Vendor	pom	developer name	Tim OBrien	Medium
Vendor	pom	groupid	org.apache.commons	Highest
Vendor	pom	name	Apache Commons Digester	High
Vendor	pom	parent-artifactid	commons-parent	Low
Vendor	pom	url	http://commons.apache.org/digester/	Highest
Product	file	name	commons-digester3	High
Product	jar	package name	apache	Highest
Product	jar	package name	commons	Highest
Product	jar	package name	digester	Highest
Product	jar	package name	digester3	Highest
Product	jar	package name	rules	Highest
Product	Manifest	bundle-docurl	http://commons.apache.org/digester/	Low
Product	Manifest	Bundle-Name	Apache Commons Digester	Medium
Product	Manifest	bundle-symbolicname	org.apache.commons.digester	Medium
Product	Manifest	implementation-build	tags/DIGESTER3_3_2_RC2@r1212807; 2011-12-10 15:57:06+0100	Low
Product	Manifest	Implementation-Title	Apache Commons Digester	High

Product	Manifest	specification-title	Apache Commons Digester	Medium
Product	pom	artifactid	commons-digester3	Highest
Product	pom	developer email	craigmcc@apache.org	Low
Product	pom	developer email	jfarcand@apache.org	Low
Product	pom	developer email	jstrachan@apache.org	Low
Product	pom	developer email	jvanzyl@apache.org	Low
Product	pom	developer email	mbenson AT apache DOT org	Low
Product	pom	developer email	rahul AT apache DOT org	Low
Product	pom	developer email	rdonkin@apache.org	Low
Product	pom	developer email	sanders@totalsync.com	Low
Product	pom	developer email	simonetripodi AT apache DOT org	Low
Product	pom	developer email	skitching@apache.org	Low
Product	pom	developer email	tobrien@apache.org	Low
Product	pom	developer id	craigmcc	Low
Product	pom	developer id	jfarcand	Low
Product	pom	developer id	jstrachan	Low
Product	pom	developer id	jvanzyl	Low
Product	pom	developer id	mbenson	Low
Product	pom	developer id	rahul	Low
Product	pom	developer id	rdonkin	Low
Product	pom	developer id	sanders	Low
Product	pom	developer id	simonetripodi	Low
Product	pom	developer id	skitching	Low
Product	pom	developer id	tobrien	Low
Product	pom	developer name	Craig McClanahan	Low
Product	pom	developer name	James Strachan	Low
Product	pom	developer name	Jason van Zyl	Low
Product	pom	developer name	Jean-Francois Arcand	Low
Product	pom	developer name	Matt Benson	Low
Product	pom	developer name	Rahul Akolkar	Low
Product	pom	developer name	Robert Burrell Donkin	Low
Product	pom	developer name	Scott Sanders	Low
Product	pom	developer name	Simon Kitching	Low
Product	pom	developer name	Simone Tripodi	Low
Product	pom	developer name	Tim OBrien	Low

Product	pom	groupid	org.apache.commons	Highest
Product	pom	name	Apache Commons Digester	High
Product	pom	parent-artifactid	commons-parent	Medium
Product	pom	url	http://commons.apache.org/digester/	Medium
Version	Manifest	Implementation-Version	3.2	High
Version	pom	parent-version	3.2	Low
Version	pom	version	3.2	Highest

Identifiers

- pkg:maven/org.apache.commons/commons-digester3@3.2 (*Confidence*:High)

help.zip: help.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/help.jar
MD5: f37950da6f8a67b745debe01fb9cb1d1
SHA1: 9a251c3847cdcacf067ece128069f4d67439bd10
SHA256:2653498bc5866cca19580be0d4d253e3e53ba88006f2c53368757a363ed7c5c0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	help	High
Vendor	jar	package name	help	Low
Vendor	jar	package name	inet	Low
Vendor	Manifest	built-date	2026-09-28 17:33	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	help	High
Product	jar	package name	help	Highest

Product	jar	package name	help	Low
Product	Manifest	built-date	2026-09-28 17:33	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	help	High
Product	Manifest	specification-title	help	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

help.zip: help.jar: ai-search.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/help.jar/com/inet/help/resources/js/ai-search.js
MD5: 67988e7a48d7694191ae33c84b3fdaf4
SHA1: 2768cd857b373bbc76caac7bc1fe1f078e9c3aed
SHA256:6136577a1f632fbc041e042460562c554c9c2c6a3f67ae08ac1e3e573e3c95bf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

help.zip: help.jar: app.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/help.jar/com/inet/help/resources/js/app.js
MD5: 3a626c6ba8ee31fb8ebf60eabda6f994
SHA1: c39bfbdd57aadcb966452b9fc2790e555fa12867
SHA256:1a77be335c5f6949c202f5b8e959c01b7d20c29d70b1fa242805724dc08a5f71
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

help.zip: help.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/help.jar/com/inet/help/resources/js/controller.js
MD5: d8a97347f09fb6127724e1fb9eaff6db
SHA1: e5c022756b372c39a872de0429fe106283dcab6d
SHA256:87e3ee1681a99819dc61cbff19258371a350cd8d7e1ca570d572a5850968a41b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

help.zip: help.jar: shared.factory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/help.jar/com/inet/help/resources/js/shared.factory.js
MD5: 0b9f1c69fe745940b59dfcc46b07c9e8
SHA1: d04efd9797d2fdca767d508cf120351bef141846
SHA256:1b2cc4f4fd954ea4954b04681293f059a417fe38c59c129f87bd22dbc9bdf0cc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

help.zip: help.jar: shared.highlighter.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/help.jar/com/inet/help/resources/js/shared.highlighter.js
MD5: af91e703b72f064acb7b0980a1981705
SHA1: 53a2a1c5190b1f3a3e3d4e68e645a152732c1893
SHA256:12e9a91bfad9c6958f82cc85b396c869363b181054843e472342bad54ebd4ad1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

help.zip: jsoup.jar

Description:

jsoup is a Java library that simplifies working with real-world HTML and XML. It offers an easy-to-use API for URL fetching, data parsing, extraction, and manipulation using DOM API methods, CSS, and xpath selectors. jsoup implements the WHATWG HTML5 specification, and parses HTML to the same DOM as modern browsers.

License:

The MIT License: https://jsoup.org/license

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/help.zip/jsoup.jar
MD5: dad42fe034bdd1636381520a957e628c
SHA1: 0c0350bb325da274f0508349109516a7855d01ab
SHA256:8b15e2b28eeb1e0a88a9b7dab4dc0c23524491c56959785dea22f7846897b668
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jsoup	High
Vendor	jar	package name	jsoup	Highest

Vendor	jar	package name	org	Highest
Vendor	jar	package name	parser	Highest
Vendor	Manifest	build-jdk-spec	17	Low
Vendor	Manifest	bundle-docurl	https://jsoup.org/	Low
Vendor	Manifest	bundle-symbolicname	org.jsoup	Medium
Vendor	Manifest	Implementation-Vendor	Jonathan Hedley	High
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	originally-created-by	Apache Maven Bundle Plugin 5.1.9	Low
Vendor	pom	artifactid	jsoup	Low
Vendor	pom	developer email	jonathan@hedley.net	Low
Vendor	pom	developer id	jhy	Medium
Vendor	pom	developer name	Jonathan Hedley	Medium
Vendor	pom	groupid	org.jsoup	Highest
Vendor	pom	name	jsoup Java HTML Parser	High
Vendor	pom	organization name	Jonathan Hedley	High
Vendor	pom	organization url	https://jhedley.com/	Medium
Vendor	pom	url	https://jsoup.org/	Highest
Product	file	name	jsoup	High
Product	jar	package name	jsoup	Highest
Product	jar	package name	org	Highest
Product	jar	package name	parser	Highest
Product	Manifest	build-jdk-spec	17	Low
Product	Manifest	bundle-docurl	https://jsoup.org/	Low
Product	Manifest	Bundle-Name	jsoup Java HTML Parser	Medium
Product	Manifest	bundle-symbolicname	org.jsoup	Medium
Product	Manifest	Implementation-Title	jsoup Java HTML Parser	High
Product	Manifest	multi-release	true	Low
Product	Manifest	originally-created-by	Apache Maven Bundle Plugin 5.1.9	Low
Product	pom	artifactid	jsoup	Highest
Product	pom	developer email	jonathan@hedley.net	Low
Product	pom	developer id	jhy	Low
Product	pom	developer name	Jonathan Hedley	Low

Product	pom	groupid	org.jsoup	Highest
Product	pom	name	jsoup Java HTML Parser	High
Product	pom	organization name	Jonathan Hedley	Low
Product	pom	organization url	https://jhedley.com/	Low
Product	pom	url	https://jsoup.org/	Medium
Version	Manifest	Bundle-Version	1.23.1	High
Version	Manifest	Implementation-Version	1.23.1	High
Version	pom	version	1.23.1	Highest

Identifiers

- pkg:maven/org.jsoup/jsoup@1.23.1 (*Confidence*:High)
- cpe:2.3:a:jsoup:jsoup:1.23.1:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

htmlengine.zip: JWebEngine.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/htmlengine.zip/JWebEngine.jar
MD5: 177e63ba90aa48f15d468a17709798cc
SHA1: 3345353b1fd00d6071e5dbb38d072309361f62c3
SHA256:bfa6f81e8cd8f01413104f416d4e28db279eb57fab78810a25cfbd6cbad3f0c1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	JWebEngine	High
Vendor	jar	package name	html	Low
Vendor	jar	package name	inet	Low
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	built-date	2026-09-28 01:24	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	implementation-group	lib	Low
Vendor	Manifest	Implementation-	i-net software	High

		Vendor		
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	trusted-library	false	Low
Vendor	Manifest	trusted-only	false	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	JWebEngine	High
Product	jar	package name	html	Low
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	built-date	2026-09-28 01:24	Low
Product	Manifest	codebase	*	Low
Product	Manifest	implementation-group	lib	Low
Product	Manifest	Implementation-Title	JWebEngine	High
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	specification-title	JWebEngine	Medium
Product	Manifest	trusted-library	false	Low
Product	Manifest	trusted-only	false	Low
Version	Manifest	Implementation-Version	1.14.315	High

Identifiers

- **None**

htmlengine.zip: htmlengine.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/htmlengine.zip/htmlengine.jar
MD5: 5df6071727c6dc54e72019bfa7215c73
SHA1: 8454027ad7a6b717f945cf2b948947e6b91c001d
SHA256:c43b2033a583ee6e0219caab4f6fdb0402911b4a907b67c5581cfedfa1e7d1c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	htmlengine	High
Vendor	jar	package name	api	Low
Vendor	jar	package name	htmlengine	Low
Vendor	jar	package name	inet	Low
Vendor	Manifest	built-date	2026-09-28 17:46	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	htmlengine	High
Product	jar	package name	api	Low
Product	jar	package name	htmlengine	Highest
Product	jar	package name	htmlengine	Low
Product	jar	package name	markdown	Low
Product	Manifest	built-date	2026-09-28 17:46	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	htmlengine	High
Product	Manifest	specification-title	htmlengine	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

inetcore-26.10-tools.jar

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/shared/inetcore/26.10/30501aa2b290db2c08431a5f481dff662ccc483b/inetcore-26.10-tools.jar
MD5: 7ea88a60fac4fca4caccc3e13b7466ed
SHA1: 30501aa2b290db2c08431a5f481dff662ccc483b
SHA256:fc11935e57381c46af3208ddda282b7e13c9bb4845c9265a7d6180548402ec8e
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	inetcore	High
Vendor	gradle	artifactid	inetcore	Highest
Vendor	gradle	groupid	shared	Highest
Vendor	jar	package name	test	Low
Vendor	Manifest	classifier	tools	Low
Product	file	name	inetcore	High
Product	gradle	artifactid	inetcore	Highest
Product	jar	package name	tools	Highest
Product	Manifest	classifier	tools	Low
Version	file	name	inetcore	Medium
Version	file	version	26.10	High
Version	gradle	version	26.10	Highest
Version	jar	package name	tools	Highest
Version	Manifest	specification-version	26.10.199	High

Identifiers

- pkg:maven/shared/inetcore@26.10 (*Confidence*:Highest)

inetcore-26.10.jar (shaded: com.inet.shared:inetcore:null)

Description:

A blend composite defines the rule according to which a drawing primitive (known as the source) is mixed with existing graphics (know as the destination.)

ColorUtilities contains a set of tools to perform common color operations easily.

License:

LGPL: http://www.gnu.org/licenses/lgpl.txt

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/shared/inetcore/26.10/a65fcaf31339e0655606ebc102774e1ab01e7994/inetcore-26.10.jar/META-INF/com/inet/shared/utils/BlendComposite/pom.xml
MD5: 15e3963148212192804e2b1a2b73ad1c
SHA1: 1095ba4522949a04590ab9c98b7f684e92579ef9
SHA256:e5556987ad0b1ede84a994741147dadf6de0cb7d80b845f530e2a96505b79151
Referenced In Projects/Scopes:

- CoWorkInstaller
- CoWorkInstaller:inetPlugin

Evidence

Type	Source	Name	Value	Confidence
Vendor	pom	artifactid	inetcore	Low
Vendor	pom	developer email	contact@inetsoftware.de	Low
Vendor	pom	developer email	morgand@apache.org	Low
Vendor	pom	developer id	inetsoftware	Medium
Vendor	pom	developer id	romainguy	Medium
Vendor	pom	developer id	sun	Medium
Vendor	pom	developer name	i-net /// software	Medium
Vendor	pom	developer name	Romain Guy	Medium
Vendor	pom	developer name	Sun	Medium
Vendor	pom	developer org	Sun	Medium
Vendor	pom	groupid	com.inet.shared	Highest
Vendor	pom	name	BlendComposite and ColorUtilities	High
Vendor	pom (hint)	developer id	oracle	Medium
Vendor	pom (hint)	developer name	oracle	Medium
Vendor	pom (hint)	developer org	oracle	Medium
Product	pom	artifactid	inetcore	Highest
Product	pom	developer email	contact@inetsoftware.de	Low
Product	pom	developer email	morgand@apache.org	Low
Product	pom	developer id	inetsoftware	Low
Product	pom	developer id	romainguy	Low
Product	pom	developer id	sun	Low
Product	pom	developer name	i-net /// software	Low
Product	pom	developer name	Romain Guy	Low
Product	pom	developer name	Sun	Low

Product	pom	developer org	Sun	Low
Product	pom	groupid	com.inet.shared	Highest
Product	pom	name	BlendComposite and ColorUtilities	High

Identifiers

- **None**

inetcore-26.10.jar

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/shared/inetcore/26.10/a65fcaf31339e0655606ebc102774e1ab01e7994/inetcore-26.10.jar
MD5: 82b83a8f2d28968e0934442eaf305880
SHA1: a65fcaf31339e0655606ebc102774e1ab01e7994
SHA256:50f38e1eef4c5bd138743acccc1029924b068c0d407f2da683028c5f8c01ca21
Referenced In Projects/Scopes:

- CoWorkInstaller
- CoWorkInstaller:inetPlugin

Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	inetcore	High
Vendor	gradle	artifactid	inetcore	Highest
Vendor	gradle	groupid	shared	Highest
Vendor	jar	package name	i	Highest
Vendor	jar	package name	inet	Low
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	built-date	2026-09-28 17:02	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium

Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	trusted-library	false	Low
Vendor	Manifest	trusted-only	false	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	inetcore	High
Product	gradle	artifactid	inetcore	Highest
Product	jar	package name	permissions	Highest
Product	jar	package name	shared	Highest
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	built-date	2026-09-28 17:02	Low
Product	Manifest	codebase	*	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	inetcore	High
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	specification-title	inetcore	Medium
Product	Manifest	trusted-library	false	Low
Product	Manifest	trusted-only	false	Low
Version	file	name	inetcore	Medium
Version	file	version	26.10	High
Version	gradle	version	26.10	Highest
Version	jar	package name	permissions	Highest
Version	jar	package name	shared	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Related Dependencies

- inetcore.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/inetcore.jar
  - MD5: 82b83a8f2d28968e0934442eaf305880
  - SHA1: a65fcaf31339e0655606ebc102774e1ab01e7994
  - SHA256: 50f38e1eef4c5bd138743acccc1029924b068c0d407f2da683028c5f8c01ca21

Identifiers

- pkg:maven/shared/inetcore@26.10 (*Confidence*:Highest)

inetloggeradapter.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/inetloggeradapter.jar
MD5: 08d4a13af7a61fc7ec4305b6f8381d4a
SHA1: 62d848b2bb981a6560e181fe90cc62323f90c4ba
SHA256:2e013c78a354dec846bb1b528d0343881aec43efa63f05dfd17b7f5a49694757
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	inetloggeradapter	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	slf4j	Low
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	built-date	2026-09-28 17:20	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	trusted-library	false	Low
Vendor	Manifest	trusted-only	false	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	inetloggeradapter	High
Product	jar	package name	slf4j	Low
Product	Manifest	application-library-allowable-	*	Low

		codebase		
Product	Manifest	built-date	2026-09-28 17:20	Low
Product	Manifest	codebase	*	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	i-net Logger Adapter	High
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	specification-title	inetloggeradapter	Medium
Product	Manifest	trusted-library	false	Low
Product	Manifest	trusted-only	false	Low
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

jakarta.servlet-api.jar

Description:

Jakarta Servlet 6.1

License:

EPL 2.0: http://www.eclipse.org/legal/epl-2.0
GPL2 w/ CPE: https://www.gnu.org/software/classpath/license.html

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/jakarta.servlet-api.jar
MD5: 314c930b3e40ac1abc3529c7c9942f09
SHA1: 1169a246913fe3823782af7943e7a103634867c5
SHA256:8a31f465f3593bf2351531a5c952014eb839da96a605b5825b93dd54714c48c4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jakarta.servlet-api	High
Vendor	jar	package name	jakarta	Highest
Vendor	jar	package name	servlet	Highest
Vendor	Manifest	build-jdk-spec	11	Low

Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low
Vendor	Manifest	bundle-symbolicname	jakarta.servlet-api	Medium
Vendor	Manifest	extension-name	jakarta.servlet	Medium
Vendor	Manifest	Implementation-Vendor	Eclipse Foundation	High
Vendor	Manifest	Implementation-Vendor-Id	org.eclipse	Medium
Vendor	Manifest	specification-vendor	Eclipse Foundation	Low
Vendor	pom	artifactid	jakarta.servlet-api	Low
Vendor	pom	developer id	yaminikb	Medium
Vendor	pom	developer name	Yamini K B	Medium
Vendor	pom	developer org	Oracle Corporation	Medium
Vendor	pom	developer org URL	http://www.oracle.com/	Medium
Vendor	pom	groupid	jakarta.servlet	Highest
Vendor	pom	name	Jakarta Servlet	High
Vendor	pom	parent-artifactid	project	Low
Vendor	pom	parent-groupid	org.eclipse.ee4j	Medium
Vendor	pom	url	https://projects.eclipse.org/projects/ee4j.servlet	Highest
Product	file	name	jakarta.servlet-api	High
Product	jar	package name	jakarta	Highest
Product	jar	package name	servlet	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Jakarta Servlet	Medium
Product	Manifest	bundle-symbolicname	jakarta.servlet-api	Medium
Product	Manifest	extension-name	jakarta.servlet	Medium
Product	pom	artifactid	jakarta.servlet-api	Highest
Product	pom	developer id	yaminikb	Low
Product	pom	developer name	Yamini K B	Low
Product	pom	developer org	Oracle Corporation	Low
Product	pom	developer org URL	http://www.oracle.com/	Low
Product	pom	groupid	jakarta.servlet	Highest
Product	pom	name	Jakarta Servlet	High

Product	pom	parent-artifactid	project	Medium
Product	pom	parent-groupid	org.eclipse.ee4j	Medium
Product	pom	url	https://projects.eclipse.org/projects/ee4j.servlet	Medium
Version	Manifest	Bundle-Version	6.1.0	High
Version	Manifest	Implementation-Version	6.1.0	High
Version	pom	parent-version	6.1.0	Low
Version	pom	version	6.1.0	Highest

Identifiers

- pkg:maven/jakarta.servlet/jakarta.servlet-api@6.1.0 (*Confidence*:High)

jakarta.websocket-api.jar

Description:

Jakarta WebSocket - Server API

License:

https://www.eclipse.org/org/documents/epl-2.0/EPL-2.0.txt, https://www.gnu.org/software/classpath/license.html

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/jakarta.websocket-api.jar
MD5: b1098129a9c74ae03d618fb841990ab0
SHA1: 60e525188fdb42120506debd90ffd4e204fd6f24
SHA256:541d00436cbca0a5e1f6a457c9f70a64f00bd2f83e10ed89c2b372bc34843b7e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jakarta.websocket-api	High
Vendor	jar	package name	jakarta	Highest
Vendor	jar	package name	server	Highest
Vendor	jar	package name	websocket	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low
Vendor	Manifest	bundle-symbolicname	jakarta.websocket-api	Medium

Vendor	Manifest	extension-name	jakarta.websocket	Medium
Vendor	Manifest	Implementation-Vendor	Eclipse Foundation	High
Vendor	Manifest	specification-vendor	Eclipse Foundation	Low
Vendor	pom	artifactid	jakarta.websocket-api	Low
Vendor	pom	groupid	jakarta.websocket	Highest
Vendor	pom	name	Jakarta WebSocket - Server API	High
Vendor	pom	parent-artifactid	jakarta.websocket-all	Low
Vendor	pom	url	https://projects.eclipse.org/projects/ee4j.websocket	Highest
Product	file	name	jakarta.websocket-api	High
Product	jar	package name	jakarta	Highest
Product	jar	package name	server	Highest
Product	jar	package name	websocket	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Jakarta WebSocket - Server API	Medium
Product	Manifest	bundle-symbolicname	jakarta.websocket-api	Medium
Product	Manifest	extension-name	jakarta.websocket	Medium
Product	pom	artifactid	jakarta.websocket-api	Highest
Product	pom	groupid	jakarta.websocket	Highest
Product	pom	name	Jakarta WebSocket - Server API	High
Product	pom	parent-artifactid	jakarta.websocket-all	Medium
Product	pom	url	https://projects.eclipse.org/projects/ee4j.websocket	Medium
Version	Manifest	Bundle-Version	2.2.0	High
Version	Manifest	Implementation-Version	2.2.0	High
Version	pom	version	2.2.0	Highest

Identifiers

- pkg:maven/jakarta.websocket/jakarta.websocket-api@2.2.0 (*Confidence*:High)

jakarta.websocket-client-api.jar

Description:

Jakarta WebSocket - Client API

License:

https://www.eclipse.org/org/documents/epl-2.0/EPL-2.0.txt, https://www.gnu.org/software/classpath/license.html

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/jakarta.websocket-client-api.jar
MD5: 9c363a8d4ab7b78b6160569e27568c1a
SHA1: cf7eafc1b929a80429c77e4450c6720a7de56814
SHA256:aa6fa9331a3f470daee0dbfcf084abfbd7a49507297575d5bb8bfbf3d62fe8c0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jakarta.websocket-client-api	High
Vendor	jar	package name	jakarta	Highest
Vendor	jar	package name	websocket	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low
Vendor	Manifest	bundle-symbolicname	jakarta.websocket-client-api	Medium
Vendor	Manifest	extension-name	jakarta.websocket-client	Medium
Vendor	Manifest	Implementation-Vendor	Eclipse Foundation	High
Vendor	Manifest	specification-vendor	Eclipse Foundation	Low
Vendor	pom	artifactid	jakarta.websocket-client-api	Low
Vendor	pom	groupid	jakarta.websocket	Highest
Vendor	pom	name	Jakarta WebSocket - Client API	High
Vendor	pom	parent-artifactid	jakarta.websocket-all	Low
Vendor	pom	url	https://projects.eclipse.org/projects/ee4j.websocket	Highest
Product	file	name	jakarta.websocket-client-api	High
Product	jar	package name	jakarta	Highest
Product	jar	package name	websocket	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Jakarta WebSocket - Client API	Medium
Product	Manifest	bundle-	jakarta.websocket-client-api	Medium

		symbolicname		
Product	Manifest	extension-name	jakarta.websocket-client	Medium
Product	pom	artifactid	jakarta.websocket-client-api	Highest
Product	pom	groupid	jakarta.websocket	Highest
Product	pom	name	Jakarta WebSocket - Client API	High
Product	pom	parent-artifactid	jakarta.websocket-all	Medium
Product	pom	url	https://projects.eclipse.org/projects/ee4j.websocket	Medium
Version	Manifest	Bundle-Version	2.2.0	High
Version	Manifest	Implementation-Version	2.2.0	High
Version	pom	version	2.2.0	Highest

Identifiers

- pkg:maven/jakarta.websocket/jakarta.websocket-client-api@2.2.0 (*Confidence*:High)

java-25-jre-x64-linux.tar.gz: java-25-jre-x64-linux.tar: jrt-fs.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/java-25-jre-x64-linux.tar.gz/java-25-jre-x64-linux.tar/jre-11/lib/jrt-fs.jar
MD5: 790d688cfe7f5ac37258fbf8083eb266
SHA1: 5d0b6d8366c9396dc1f759a3470c156d1608ef94
SHA256:2bd8b0fb53c9d0e240128953e6145e0bbe230168a3444c89fff81002beb60c14
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jrt-fs	High
Vendor	jar	package name	internal	Low
Vendor	jar	package name	jdk	Low
Vendor	jar	package name	jimage	Low
Vendor	Manifest	Implementation-Vendor	Eclipse Adoptium	High
Vendor	Manifest	specification-vendor	Oracle Corporation	Low
Product	file	name	jrt-fs	High
Product	jar	package name	internal	Low

Product	jar	package name	jimage	Low
Product	Manifest	Implementation-Title	Java Runtime Environment	High
Product	Manifest	specification-title	Java Platform API Specification	Medium
Version	Manifest	Implementation-Version	25.0.4	High

Identifiers

- cpe:2.3:a:eclipse:platform:25.0.4:*:*:*:*:*:*:* (*Confidence*:Medium) suppress

jcip-annotations-1.0.jar

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/net.jcip/jcip-annotations/1.0/afba4942caaeaf46aab0b976afd57cc7c181467e/jcip-annotations-1.0.jar
MD5: 9d5272954896c5a5d234f66b7372b17a
SHA1: afba4942caaeaf46aab0b976afd57cc7c181467e
SHA256:be5805392060c71474bf6c9a67a099471274d30b83eef84bfc4e0889a4f1dcc0
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/de.inetsoftware/jlessc@1.16

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jcip-annotations	High
Vendor	gradle	artifactid	jcip-annotations	Highest
Vendor	gradle	groupid	net.jcip	Highest
Vendor	jar	package name	annotations	Low
Vendor	jar	package name	jcip	Low
Vendor	jar	package name	net	Low
Vendor	pom	artifactid	jcip-annotations	Low
Vendor	pom	groupid	net.jcip	Highest
Vendor	pom	name	"Java Concurrency in Practice" book annotations	High
Vendor	pom	url	http://jcip.net/	Highest
Product	file	name	jcip-annotations	High
Product	gradle	artifactid	jcip-annotations	Highest
Product	jar	package name	annotations	Low
Product	jar	package name	jcip	Low

Product	pom	artifactid	jcip-annotations	Highest
Product	pom	groupid	net.jcip	Highest
Product	pom	name	"Java Concurrency in Practice" book annotations	High
Product	pom	url	http://jcip.net/	Medium
Version	file	version	1.0	High
Version	gradle	version	1.0	Highest
Version	pom	version	1.0	Highest

Identifiers

- pkg:maven/net.jcip/jcip-annotations@1.0 (*Confidence*:High)

jlessc-1.16.jar

Description:

A Less CSS compiler written completely in Java (pure Java).

License:

MIT License: http://www.opensource.org/licenses/mit-license.php

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/de.inetsoftware/jlessc/1.16/d2d7a35fe5daa804be79c9e77073d9b941c28a94/jlessc-1.16.jar
MD5: 0f7350b2bb443d0f0b9a8039fff69261
SHA1: d2d7a35fe5daa804be79c9e77073d9b941c28a94
SHA256:1d188752d493662c97496c178b5a6405e8168133ce7d343f4dd2f3eab470b922
Referenced In Projects/Scopes:

- CoWorkInstaller
- CoWorkInstaller:inetPlugin

Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jlessc	High
Vendor	gradle	artifactid	jlessc	Highest
Vendor	gradle	groupid	de.inetsoftware	Highest
Vendor	jar	package name	inet	Low
Vendor	jar	package name	less	Low
Vendor	jar	package name	lib	Low

Vendor	Manifest	automatic-module-name	de.inetsoftware.jlessc	Medium
Vendor	Manifest	bundle-symbolicname	de.inetsoftware.jlessc	Medium
Vendor	Manifest	Implementation-Vendor	i-net software GmbH, Berlin, Germany	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	pom	artifactid	jlessc	Low
Vendor	pom	developer email	vberlin@inetsoftware.de	Low
Vendor	pom	developer id	vberlin	Medium
Vendor	pom	developer name	Volker Berlin	Medium
Vendor	pom	developer org	i-net software	Medium
Vendor	pom	developer org URL	https://www.inetsoftware.de/	Medium
Vendor	pom	groupid	de.inetsoftware	Highest
Vendor	pom	name	JLessC	High
Vendor	pom	url	i-net-software/jlessc	Highest
Product	file	name	jlessc	High
Product	gradle	artifactid	jlessc	Highest
Product	jar	package name	less	Low
Product	jar	package name	lib	Low
Product	Manifest	automatic-module-name	de.inetsoftware.jlessc	Medium
Product	Manifest	bundle-symbolicname	de.inetsoftware.jlessc	Medium
Product	Manifest	Implementation-Title	JLessC, a Less CSS compiler	High
Product	pom	artifactid	jlessc	Highest
Product	pom	developer email	vberlin@inetsoftware.de	Low
Product	pom	developer id	vberlin	Low
Product	pom	developer name	Volker Berlin	Low
Product	pom	developer org	i-net software	Low
Product	pom	developer org URL	https://www.inetsoftware.de/	Low
Product	pom	groupid	de.inetsoftware	Highest
Product	pom	name	JLessC	High
Product	pom	url	i-net-software/jlessc	High
Version	file	version	1.16	High
Version	gradle	version	1.16	Highest

Version	Manifest	Bundle-Version	1.16	High
Version	Manifest	Implementation-Version	1.16	High
Version	pom	version	1.16	Highest

Related Dependencies

- theme.zip: jlessc.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/theme.zip/jlessc.jar
  - MD5: 0f7350b2bb443d0f0b9a8039fff69261
  - SHA1: d2d7a35fe5daa804be79c9e77073d9b941c28a94
  - SHA256: 1d188752d493662c97496c178b5a6405e8168133ce7d343f4dd2f3eab470b922

Identifiers

- pkg:maven/de.inetsoftware/jlessc@1.16 (*Confidence*:High)

jsr305-3.0.2.jar

Description:

JSR305 Annotations for Findbugs

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/com.google.code.findbugs/jsr305/3.0.2/25ea2e8b0c338a877313bd4672d3fe056ea78f0d/jsr305-3.0.2.jar
MD5: dd83accb899363c32b07d7a1b2e4ce40
SHA1: 25ea2e8b0c338a877313bd4672d3fe056ea78f0d
SHA256:766ad2a0783f2687962c8ad74ceecc38a28b9f72a2d085ee438b7813e928d0c7
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/de.inetsoftware/jlessc@1.16

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jsr305	High
Vendor	gradle	artifactid	jsr305	Highest
Vendor	gradle	groupid	com.google.code.findbugs	Highest
Vendor	Manifest	bundle-symbolicname	org.jsr-305	Medium

Vendor	pom	artifactid	jsr305	Low
Vendor	pom	groupid	com.google.code.findbugs	Highest
Vendor	pom	name	FindBugs-jsr305	High
Vendor	pom	url	http://findbugs.sourceforge.net/	Highest
Product	file	name	jsr305	High
Product	gradle	artifactid	jsr305	Highest
Product	Manifest	Bundle-Name	FindBugs-jsr305	Medium
Product	Manifest	bundle-symbolicname	org.jsr-305	Medium
Product	pom	artifactid	jsr305	Highest
Product	pom	groupid	com.google.code.findbugs	Highest
Product	pom	name	FindBugs-jsr305	High
Product	pom	url	http://findbugs.sourceforge.net/	Medium
Version	file	version	3.0.2	High
Version	gradle	version	3.0.2	Highest
Version	Manifest	Bundle-Version	3.0.2	High
Version	pom	version	3.0.2	Highest

Identifiers

- pkg:maven/com.google.code.findbugs/jsr305@3.0.2 (*Confidence*:High)

junit-4.13.2.jar

Description:

JUnit is a unit testing framework for Java, created by Erich Gamma and Kent Beck.

License:

Eclipse Public License 1.0: http://www.eclipse.org/legal/epl-v10.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/junit/junit/4.13.2/8ac9e16d933b6fb43bc7f576336b8f4d7eb5ba12/junit-4.13.2.jar
MD5: d98a9a02a99a9acd22d7653cbcc1f31f
SHA1: 8ac9e16d933b6fb43bc7f576336b8f4d7eb5ba12
SHA256:8e495b634469d64fb8acfa3495a065cbacc8a0fff55ce1e31007be4c16dc57d3
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit	High
Vendor	gradle	artifactid	junit	Highest
Vendor	gradle	groupid	junit	Highest
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	Manifest	automatic-module-name	junit	Medium
Vendor	Manifest	implementation-url	http://junit.org	Low
Vendor	Manifest	Implementation-Vendor	JUnit	High
Vendor	Manifest	Implementation-Vendor-Id	junit	Medium
Vendor	pom	artifactid	junit	Low
Vendor	pom	developer email	david@saff.net	Low
Vendor	pom	developer email	kcooney@google.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	mail@stefan-birkner.de	Low
Vendor	pom	developer id	dsaff	Medium
Vendor	pom	developer id	kcooney	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	stefanbirkner	Medium
Vendor	pom	developer name	David Saff	Medium
Vendor	pom	developer name	Kevin Cooney	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Stefan Birkner	Medium
Vendor	pom	groupid	junit	Highest
Vendor	pom	name	JUnit	High
Vendor	pom	organization name	JUnit	High
Vendor	pom	organization url	http://www.junit.org	Medium
Vendor	pom	url	http://junit.org	Highest
Product	file	name	junit	High
Product	gradle	artifactid	junit	Highest
Product	jar	package name	junit	Highest
Product	Manifest	automatic-module-name	junit	Medium

Product	Manifest	Implementation-Title	JUnit	High
Product	Manifest	implementation-url	http://junit.org	Low
Product	pom	artifactid	junit	Highest
Product	pom	developer email	david@saff.net	Low
Product	pom	developer email	kcooney@google.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	mail@stefan-birkner.de	Low
Product	pom	developer id	dsaff	Low
Product	pom	developer id	kcooney	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	stefanbirkner	Low
Product	pom	developer name	David Saff	Low
Product	pom	developer name	Kevin Cooney	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Stefan Birkner	Low
Product	pom	groupid	junit	Highest
Product	pom	name	JUnit	High
Product	pom	organization name	JUnit	Low
Product	pom	organization url	http://www.junit.org	Low
Product	pom	url	http://junit.org	Medium
Version	file	version	4.13.2	High
Version	gradle	version	4.13.2	Highest
Version	Manifest	Implementation-Version	4.13.2	High
Version	pom	version	4.13.2	Highest

Identifiers

- pkg:maven/junit/junit@4.13.2 (*Confidence*:High)
- cpe:2.3:a:junit:junit4:4.13.2:*:*:*:*:*:*:* (*Confidence*:Low) suppress

junit-jupiter-6.1.3.jar

Description:

Module "junit-jupiter" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.jupiter/junit-jupiter/6.1.3/cd72619e9eb4cf64e30a87615a4f9b50a80ce103/junit-jupiter-6.1.3.jar
MD5: ce9a15168b49704e731f11120d5dc1b9
SHA1: cd72619e9eb4cf64e30a87615a4f9b50a80ce103
SHA256:6b0a14075c74221de53047e363860b7d19fce802bebc152df2c35c4089c6c379
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/cowork/CoWorkInstaller@26.10
- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-jupiter	High
Vendor	gradle	artifactid	junit-jupiter	Highest
Vendor	gradle	groupid	org.junit.jupiter	Highest
Vendor	jar	package name	module-info	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-jupiter	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-jupiter	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium

Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.jupiter	Highest
Vendor	pom	name	JUnit Jupiter (Aggregator)	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-jupiter	High
Product	gradle	artifactid	junit-jupiter	Highest
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Jupiter (Aggregator)	Medium
Product	Manifest	bundle-symbolicname	junit-jupiter	Medium
Product	Manifest	Implementation-Title	junit-jupiter	High
Product	Manifest	specification-title	junit-jupiter	Medium
Product	pom	artifactid	junit-jupiter	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low

Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.jupiter	Highest
Product	pom	name	JUnit Jupiter (Aggregator)	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3 (*Confidence*:High)

junit-jupiter-api-6.1.3.jar

Description:

Module "junit-jupiter-api" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.jupiter/junit-jupiter-api/6.1.3/6a57f0ce4d6bfe9784d103077055ba39f3e6f638/junit-jupiter-api-6.1.3.jar
MD5: 662a5b10a1bbb2e3192790351d67d269
SHA1: 6a57f0ce4d6bfe9784d103077055ba39f3e6f638
SHA256:555d6cf20fa1710884dd01b86cc5785397ba73e21ada2d4b784f5f1a14dcafc4
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-jupiter-api	High
Vendor	gradle	artifactid	junit-jupiter-api	Highest
Vendor	gradle	groupid	org.junit.jupiter	Highest
Vendor	jar	package name	api	Highest
Vendor	jar	package name	api	Low
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	jupiter	Highest
Vendor	jar	package name	jupiter	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-jupiter-api	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-jupiter-api	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low

Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.jupiter	Highest
Vendor	pom	name	JUnit Jupiter API	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-jupiter-api	High
Product	gradle	artifactid	junit-jupiter-api	Highest
Product	jar	package name	api	Highest
Product	jar	package name	api	Low
Product	jar	package name	junit	Highest
Product	jar	package name	jupiter	Highest
Product	jar	package name	jupiter	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Jupiter API	Medium
Product	Manifest	bundle-symbolicname	junit-jupiter-api	Medium
Product	Manifest	Implementation-	junit-jupiter-api	High

		Title		
Product	Manifest	specification-title	junit-jupiter-api	Medium
Product	pom	artifactid	junit-jupiter-api	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.jupiter	Highest
Product	pom	name	JUnit Jupiter API	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.jupiter/junit-jupiter-api@6.1.3 (*Confidence*:High)

junit-jupiter-engine-6.1.3.jar

Description:

Module "junit-jupiter-engine" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.jupiter/junit-jupiter-engine/6.1.3/3778a548f15693db463c3d090b419c64b486b848/junit-jupiter-engine-6.1.3.jar
MD5: ecb46f02088bb27be8ae3a7f51eded39
SHA1: 3778a548f15693db463c3d090b419c64b486b848
SHA256:414559e78bbfa3bdb2eab009ac3ab1e22369ac31117c270a0bd666da115c5c6c
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/cowork/CoWorkInstaller@26.10
- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-jupiter-engine	High
Vendor	gradle	artifactid	junit-jupiter-engine	Highest
Vendor	gradle	groupid	org.junit.jupiter	Highest
Vendor	jar	package name	engine	Highest
Vendor	jar	package name	engine	Low
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	jupiter	Highest
Vendor	jar	package name	jupiter	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-jupiter-engine	Medium

Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	provide-capability	org.junit.platform.engine;org.junit.platform.engine=junit-jupiter;version:Version="6.1.3"	Low
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-jupiter-engine	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.jupiter	Highest
Vendor	pom	name	JUnit Jupiter Engine	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-jupiter-engine	High
Product	gradle	artifactid	junit-jupiter-engine	Highest
Product	jar	package name	engine	Highest

Product	jar	package name	engine	Low
Product	jar	package name	junit	Highest
Product	jar	package name	jupiter	Highest
Product	jar	package name	jupiter	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Jupiter Engine	Medium
Product	Manifest	bundle-symbolicname	junit-jupiter-engine	Medium
Product	Manifest	Implementation-Title	junit-jupiter-engine	High
Product	Manifest	provide-capability	org.junit.platform.engine;org.junit.platform.engine=junit-jupiter;version:Version="6.1.3"	Low
Product	Manifest	specification-title	junit-jupiter-engine	Medium
Product	pom	artifactid	junit-jupiter-engine	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low

Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.jupiter	Highest
Product	pom	name	JUnit Jupiter Engine	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3 (*Confidence*:High)

junit-jupiter-params-6.1.3.jar

Description:

Module "junit-jupiter-params" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.jupiter/junit-jupiter-params/6.1.3/435fa4ec654c11fb82e666a47d9baefcee3f8df6/junit-jupiter-params-6.1.3.jar
MD5: e0b4bd2b6ae43ccb74acccc2b007cf6e
SHA1: 435fa4ec654c11fb82e666a47d9baefcee3f8df6
SHA256:05c51cedba2c06a9770707391e006cee825876937dea580b94a265ce145d4939
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-jupiter-params	High
Vendor	gradle	artifactid	junit-jupiter-params	Highest

Vendor	gradle	groupid	org.junit.jupiter	Highest
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	jupiter	Highest
Vendor	jar	package name	jupiter	Low
Vendor	jar	package name	params	Highest
Vendor	jar	package name	params	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-jupiter-params	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-jupiter-params	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium

Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.jupiter	Highest
Vendor	pom	name	JUnit Jupiter Params	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-jupiter-params	High
Product	gradle	artifactid	junit-jupiter-params	Highest
Product	jar	package name	junit	Highest
Product	jar	package name	jupiter	Highest
Product	jar	package name	jupiter	Low
Product	jar	package name	params	Highest
Product	jar	package name	params	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Jupiter Params	Medium
Product	Manifest	bundle-symbolicname	junit-jupiter-params	Medium
Product	Manifest	Implementation-Title	junit-jupiter-params	High
Product	Manifest	specification-title	junit-jupiter-params	Medium
Product	pom	artifactid	junit-jupiter-params	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low

Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.jupiter	Highest
Product	pom	name	JUnit Jupiter Params	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.jupiter/junit-jupiter-params@6.1.3 (*Confidence*:High)

junit-platform-commons-6.1.3.jar

Description:

Module "junit-platform-commons" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.platform/junit-platform-commons/6.1.3/acb99d3482ea51fcbcc4f6ea8672761e2b3d5bb7/junit-platform-commons-6.1.3.jar

MD5: 481a56275fe36dc163df005113a39f44
SHA1: acb99d3482ea51fcbcc4f6ea8672761e2b3d5bb7
SHA256:a4774ae923c109544034aeae7c762cf017fbcdd1342403ba90e0921984b608c3
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-platform-commons	High
Vendor	gradle	artifactid	junit-platform-commons	Highest
Vendor	gradle	groupid	org.junit.platform	Highest
Vendor	jar	package name	commons	Highest
Vendor	jar	package name	commons	Low
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	platform	Highest
Vendor	jar	package name	platform	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-platform-commons	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-platform-commons	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium

Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.platform	Highest
Vendor	pom	name	JUnit Platform Commons	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-platform-commons	High
Product	gradle	artifactid	junit-platform-commons	Highest
Product	jar	package name	commons	Highest
Product	jar	package name	commons	Low
Product	jar	package name	junit	Highest
Product	jar	package name	platform	Highest
Product	jar	package name	platform	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Platform Commons	Medium
Product	Manifest	bundle-symbolicname	junit-platform-commons	Medium
Product	Manifest	Implementation-Title	junit-platform-commons	High
Product	Manifest	specification-title	junit-platform-commons	Medium
Product	pom	artifactid	junit-platform-commons	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low

Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.platform	Highest
Product	pom	name	JUnit Platform Commons	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.platform/junit-platform-commons@6.1.3 (*Confidence*:High)

- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress

junit-platform-engine-6.1.3.jar

Description:

Module "junit-platform-engine" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.platform/junit-platform-engine/6.1.3/e48a6061b576ebe36eac3b518dc917c23d119a91/junit-platform-engine-6.1.3.jar
MD5: a8f3d8fb44590fdee64b1b56b004f45a
SHA1: e48a6061b576ebe36eac3b518dc917c23d119a91
SHA256:21ad7ad3a35beda16387979317be1833a72a71d812f9a66ee4b9a7bafb56334c
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-platform-engine	High
Vendor	gradle	artifactid	junit-platform-engine	Highest
Vendor	gradle	groupid	org.junit.platform	Highest
Vendor	jar	package name	engine	Highest
Vendor	jar	package name	engine	Low
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	platform	Highest
Vendor	jar	package name	platform	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-platform-engine	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-	junit.org	Low

		vendor		
Vendor	pom	artifactid	junit-platform-engine	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.platform	Highest
Vendor	pom	name	JUnit Platform Engine API	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-platform-engine	High
Product	gradle	artifactid	junit-platform-engine	Highest
Product	jar	package name	engine	Highest
Product	jar	package name	engine	Low
Product	jar	package name	junit	Highest
Product	jar	package name	platform	Highest

Product	jar	package name	platform	Low
Product	jar	package name	support	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Platform Engine API	Medium
Product	Manifest	bundle-symbolicname	junit-platform-engine	Medium
Product	Manifest	Implementation-Title	junit-platform-engine	High
Product	Manifest	specification-title	junit-platform-engine	Medium
Product	pom	artifactid	junit-platform-engine	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low

Product	pom	groupid	org.junit.platform	Highest
Product	pom	name	JUnit Platform Engine API	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.platform/junit-platform-engine@6.1.3 (*Confidence*:High)
- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low)

suppress

junit-platform-launcher-6.1.3.jar

Description:

Module "junit-platform-launcher" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.platform/junit-platform-launcher/6.1.3/dad54f7f53b702e6e6f873bc19903dfec870bf1b/junit-platform-launcher-6.1.3.jar
MD5: 3e91902f4602a4674f9eab70dcaa7d7a
SHA1: dad54f7f53b702e6e6f873bc19903dfec870bf1b
SHA256:1dec64b1fc0b7c47a11302aa5b4d37d8160c041b396e27067709ce775601a7b6
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-platform-launcher	High
Vendor	gradle	artifactid	junit-platform-launcher	Highest
Vendor	gradle	groupid	org.junit.platform	Highest
Vendor	jar	package name	junit	Highest

Vendor	jar	package name	junit	Low
Vendor	jar	package name	launcher	Highest
Vendor	jar	package name	launcher	Low
Vendor	jar	package name	platform	Highest
Vendor	jar	package name	platform	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-platform-launcher	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	provide-capability	org.junit.platform.launcher;org.junit.platform.launcher=junit-platform-launcher;version:Version="6.1.3"	Low
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-platform-launcher	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium

Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.platform	Highest
Vendor	pom	name	JUnit Platform Launcher	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-platform-launcher	High
Product	gradle	artifactid	junit-platform-launcher	Highest
Product	jar	package name	junit	Highest
Product	jar	package name	launcher	Highest
Product	jar	package name	launcher	Low
Product	jar	package name	platform	Highest
Product	jar	package name	platform	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Platform Launcher	Medium
Product	Manifest	bundle-symbolicname	junit-platform-launcher	Medium
Product	Manifest	Implementation-Title	junit-platform-launcher	High
Product	Manifest	provide-capability	org.junit.platform.launcher;org.junit.platform.launcher=junit-platform-launcher;version:Version="6.1.3"	Low
Product	Manifest	specification-title	junit-platform-launcher	Medium
Product	pom	artifactid	junit-platform-launcher	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low

Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.platform	Highest
Product	pom	name	JUnit Platform Launcher	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.platform/junit-platform-launcher@6.1.3 (*Confidence*:High)
- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low)

suppress

junit-platform-suite-6.1.3.jar

Description:

Module "junit-platform-suite" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.platform/junit-platform-suite/6.1.3/26278be7c21f6f64ca35e601267b68ac1f6959f2/junit-platform-suite-6.1.3.jar
MD5: 832f48fe2b81ef051c3060aae74d9994
SHA1: 26278be7c21f6f64ca35e601267b68ac1f6959f2
SHA256:cf282810206f63c6382eb3d2ff98bbfcfc31412db55397ac642849aae31e5be6
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/cowork/CoWorkInstaller@26.10
- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-platform-suite	High
Vendor	gradle	artifactid	junit-platform-suite	Highest
Vendor	gradle	groupid	org.junit.platform	Highest
Vendor	jar	package name	module-info	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-platform-suite	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-platform-suite	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium

Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.platform	Highest
Vendor	pom	name	JUnit Platform Suite (Aggregator)	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-platform-suite	High
Product	gradle	artifactid	junit-platform-suite	Highest
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Platform Suite (Aggregator)	Medium
Product	Manifest	bundle-symbolicname	junit-platform-suite	Medium
Product	Manifest	Implementation-Title	junit-platform-suite	High
Product	Manifest	specification-title	junit-platform-suite	Medium
Product	pom	artifactid	junit-platform-suite	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low

Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.platform	Highest
Product	pom	name	JUnit Platform Suite (Aggregator)	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3 (*Confidence*:High)
- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low)
  suppress

junit-platform-suite-api-6.1.3.jar

Description:

Module "junit-platform-suite-api" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.platform/junit-platform-suite-api/6.1.3/6b6577612ce5f0c11ca66db60552552fb1ea6971/junit-platform-suite-api-6.1.3.jar
MD5: d297860b330eb291100ab6b04ff4103e
SHA1: 6b6577612ce5f0c11ca66db60552552fb1ea6971
SHA256:55ee464c0846fa4a695e5c2fc8d8ea8f16fb3d92b04746831b7a428519436c11
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-platform-suite-api	High
Vendor	gradle	artifactid	junit-platform-suite-api	Highest
Vendor	gradle	groupid	org.junit.platform	Highest
Vendor	jar	package name	api	Highest
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	platform	Highest
Vendor	jar	package name	platform	Low
Vendor	jar	package name	suite	Highest
Vendor	jar	package name	suite	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-platform-suite-api	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-platform-suite-api	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low

Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.platform	Highest
Vendor	pom	name	JUnit Platform Suite API	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-platform-suite-api	High
Product	gradle	artifactid	junit-platform-suite-api	Highest
Product	jar	package name	api	Highest
Product	jar	package name	api	Low
Product	jar	package name	junit	Highest
Product	jar	package name	platform	Highest
Product	jar	package name	platform	Low
Product	jar	package name	suite	Highest
Product	jar	package name	suite	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Platform Suite API	Medium
Product	Manifest	bundle-symbolicname	junit-platform-suite-api	Medium

Product	Manifest	Implementation-Title	junit-platform-suite-api	High
Product	Manifest	specification-title	junit-platform-suite-api	Medium
Product	pom	artifactid	junit-platform-suite-api	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.platform	Highest
Product	pom	name	JUnit Platform Suite API	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High

Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.platform/junit-platform-suite-api@6.1.3 (*Confidence*:High)
- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low)

suppress

junit-platform-suite-engine-6.1.3.jar

Description:

Module "junit-platform-suite-engine" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.platform/junit-platform-suite-engine/6.1.3/720da7199a4e5766daf6e6fb4e4f2a8fdfb6e098/junit-platform-suite-engine-6.1.3.jar
MD5: 7d7a675f6b06ffe1b1bd07f3373f1578
SHA1: 720da7199a4e5766daf6e6fb4e4f2a8fdfb6e098
SHA256:6334e2ca2ac26febda4f72b1ae739661124a6cc3396448a43e72334841843e2d
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-platform-suite-engine	High
Vendor	gradle	artifactid	junit-platform-suite-engine	Highest
Vendor	gradle	groupid	org.junit.platform	Highest
Vendor	jar	package name	engine	Highest
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	platform	Highest
Vendor	jar	package name	platform	Low
Vendor	jar	package name	suite	Highest
Vendor	jar	package name	suite	Low
Vendor	Manifest	build-date	2026-08-07	Low

Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-platform-suite-engine	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-platform-suite-engine	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.platform	Highest
Vendor	pom	name	JUnit Platform Suite Engine	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-platform-suite-engine	High

Product	gradle	artifactid	junit-platform-suite-engine	Highest
Product	jar	package name	engine	Highest
Product	jar	package name	engine	Low
Product	jar	package name	junit	Highest
Product	jar	package name	platform	Highest
Product	jar	package name	platform	Low
Product	jar	package name	suite	Highest
Product	jar	package name	suite	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Platform Suite Engine	Medium
Product	Manifest	bundle-symbolicname	junit-platform-suite-engine	Medium
Product	Manifest	Implementation-Title	junit-platform-suite-engine	High
Product	Manifest	specification-title	junit-platform-suite-engine	Medium
Product	pom	artifactid	junit-platform-suite-engine	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low

Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.platform	Highest
Product	pom	name	JUnit Platform Suite Engine	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.platform/junit-platform-suite-engine@6.1.3 (*Confidence*:High)
- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low)

suppress

junit-vintage-engine-6.1.3.jar

Description:

Module "junit-vintage-engine" of JUnit

License:

Eclipse Public License v2.0: https://www.eclipse.org/legal/epl-v20.html

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.junit.vintage/junit-vintage-engine/6.1.3/ee2e019c662152a8cc983bbe0db119a5fae632b9/junit-vintage-engine-6.1.3.jar
MD5: 56538b449a01fcc6803af296edc7ae84
SHA1: ee2e019c662152a8cc983bbe0db119a5fae632b9
SHA256:37a1e6ade75c09c5385c2830b7cda21c4b1f24a5f36ed7cd7397bc40f7dc71bc
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/cowork/CoWorkInstaller@26.10
- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	junit-vintage-engine	High
Vendor	gradle	artifactid	junit-vintage-engine	Highest
Vendor	gradle	groupid	org.junit.vintage	Highest
Vendor	jar	package name	engine	Highest
Vendor	jar	package name	engine	Low
Vendor	jar	package name	junit	Highest
Vendor	jar	package name	junit	Low
Vendor	jar	package name	vintage	Highest
Vendor	jar	package name	vintage	Low
Vendor	Manifest	build-date	2026-08-07	Low
Vendor	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Vendor	Manifest	build-time	14:25:13.673+0200	Low
Vendor	Manifest	bundle-symbolicname	junit-vintage-engine	Medium
Vendor	Manifest	Implementation-Vendor	junit.org	High
Vendor	Manifest	provide-capability	org.junit.platform.engine;org.junit.platform.engine=junit-vintage;version:Version="6.1.3"	Low
Vendor	Manifest	specification-vendor	junit.org	Low
Vendor	pom	artifactid	junit-vintage-engine	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	derancourt.juliette@gmail.com	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low
Vendor	pom	developer email	mpkorstanje@junit.org	Low
Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	sormuras@gmail.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	juliette-derancourt	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	mpkorstanje	Medium

Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer id	sormuras	Medium
Vendor	pom	developer name	Christian Stein	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Juliette de Rancourt	Medium
Vendor	pom	developer name	M.P. Korstanje	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.junit.vintage	Highest
Vendor	pom	name	JUnit Vintage Engine	High
Vendor	pom	url	https://junit.org/	Highest
Product	file	name	junit-vintage-engine	High
Product	gradle	artifactid	junit-vintage-engine	Highest
Product	jar	package name	engine	Highest
Product	jar	package name	engine	Low
Product	jar	package name	junit	Highest
Product	jar	package name	vintage	Highest
Product	jar	package name	vintage	Low
Product	Manifest	build-date	2026-08-07	Low
Product	Manifest	build-revision	f59f60d2cebdf2224235d81f781b1f310cbc8138	Low
Product	Manifest	build-time	14:25:13.673+0200	Low
Product	Manifest	Bundle-Name	JUnit Vintage Engine	Medium
Product	Manifest	bundle-symbolicname	junit-vintage-engine	Medium
Product	Manifest	Implementation-Title	junit-vintage-engine	High
Product	Manifest	provide-capability	org.junit.platform.engine;org.junit.platform.engine=junit-vintage;version:Version="6.1.3"	Low
Product	Manifest	specification-title	junit-vintage-engine	Medium
Product	pom	artifactid	junit-vintage-engine	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	derancourt.juliette@gmail.com	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low

Product	pom	developer email	mpkorstanje@junit.org	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	sormuras@gmail.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	juliette-derancourt	Low
Product	pom	developer id	marcphilipp	Low
Product	pom	developer id	mmerdes	Low
Product	pom	developer id	mpkorstanje	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer id	sormuras	Low
Product	pom	developer name	Christian Stein	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Juliette de Rancourt	Low
Product	pom	developer name	M.P. Korstanje	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.junit.vintage	Highest
Product	pom	name	JUnit Vintage Engine	High
Product	pom	url	https://junit.org/	Medium
Version	file	version	6.1.3	High
Version	gradle	version	6.1.3	Highest
Version	Manifest	Bundle-Version	6.1.3	High
Version	Manifest	Implementation-Version	6.1.3	High
Version	pom	version	6.1.3	Highest

Identifiers

- pkg:maven/org.junit.vintage/junit-vintage-engine@6.1.3 (*Confidence*:High)
- cpe:2.3:a:fan_platform_project:fan_platform:6.1.3:*:*:*:*:*:*:* (*Confidence*:Low)

suppress

mail.zip: angus-activation.jar

Description:

Implementation

License:

http://www.eclipse.org/org/documents/edl-v10.php

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-activation.jar
MD5: ad20392145690b36b4f950fe31a31a2a
SHA1: 7f80607ea5014fef0b1779e6c33d63a88a45a563
SHA256:a6bd35c538cf90fff941ad6258c40c08fca0b5c9c3f536c657114f27ce0527a7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	angus-activation	High
Vendor	jar	package name	activation	Highest
Vendor	jar	package name	angus	Highest
Vendor	jar	package name	eclipse	Highest
Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low
Vendor	Manifest	bundle-symbolicname	angus-activation	Medium
Vendor	Manifest	extension-name	org.eclipse.angus	Medium
Vendor	Manifest	implementation-build-id	2.0.3-RELEASE-6eff4c5	Low
Vendor	Manifest	Implementation-Vendor	Eclipse Foundation	High
Vendor	Manifest	provide-capability	osgi.serviceloader;osgi.serviceloader="jakarta.activation.spi.MailcapRegistryProvider",osgi.serviceloader;osgi.serviceloader="jakarta.activation.spi.MimeTypeRegistryProvider"	Low
Vendor	Manifest	specification-vendor	Eclipse Foundation	Low
Vendor	pom	artifactid	angus-activation	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Activation Registries	High
Vendor	pom	parent-artifactid	angus-activation-project	Low
Product	file	name	angus-activation	High
Product	jar	package name	activation	Highest

Product	jar	package name	angus	Highest
Product	jar	package name	eclipse	Highest
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Angus Activation Registries	Medium
Product	Manifest	bundle-symbolicname	angus-activation	Medium
Product	Manifest	extension-name	org.eclipse.angus	Medium
Product	Manifest	implementation-build-id	2.0.3-RELEASE-6eff4c5	Low
Product	Manifest	Implementation-Title	Angus Activation Registries	High
Product	Manifest	provide-capability	osgi.serviceloader;osgi.serviceloader="jakarta.activation.spi.MailcapRegistryProvider",osgi.serviceloader;osgi.serviceloader="jakarta.activation.spi.MimeTypeRegistryProvider"	Low
Product	Manifest	specification-title	Jakarta Activation Specification	Medium
Product	pom	artifactid	angus-activation	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Activation Registries	High
Product	pom	parent-artifactid	angus-activation-project	Medium
Version	Manifest	Bundle-Version	2.0.3	High
Version	pom	version	2.0.3	Highest

Identifiers

- pkg:maven/org.eclipse.angus/angus-activation@2.0.3 (*Confidence*:High)

mail.zip: angus-mail.jar (shaded: org.eclipse.angus:angus-core:2.0.5)

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-mail.jar/META-INF/maven/org.eclipse.angus/angus-core/pom.xml
MD5: 102fa937d3897ac6eb838ff3a716bc80
SHA1: 11d1302ad859e7dda8e897ffa278a2135d0d3c7e
SHA256:162bec7f0c7a2c3d461a42ca576e139b80628798f97f274b7dd5759226fc47c1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Vendor	pom	artifactid	angus-core	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Mail Core	High
Vendor	pom	parent-artifactid	all	Low
Product	pom	artifactid	angus-core	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Mail Core	High
Product	pom	parent-artifactid	all	Medium
Version	pom	version	2.0.5	Highest

Identifiers

- pkg:maven/org.eclipse.angus/angus-core@2.0.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:* (*Confidence*:Low) suppress

mail.zip: angus-mail.jar (shaded: org.eclipse.angus:imap:2.0.5)

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-mail.jar/META-INF/maven/org.eclipse.angus/imap/pom.xml
MD5: c031701146f4f9887af1d7348b68e607
SHA1: bd81e3288ab646231bc2d64cedf04fe3c3146bf5
SHA256:251e848e4c2db58e57e7725434e0498043cd3d554fba21d22d5178e5783e21dd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	pom	artifactid	imap	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Mail imap provider	High
Vendor	pom	parent-artifactid	providers	Low
Product	pom	artifactid	imap	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Mail imap provider	High
Product	pom	parent-artifactid	providers	Medium
Version	pom	version	2.0.5	Highest

Identifiers

- pkg:maven/org.eclipse.angus/imap@2.0.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:* (*Confidence*:Low) suppress

mail.zip: angus-mail.jar (shaded: org.eclipse.angus:logging-mailhandler:2.0.5)

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-mail.jar/META-INF/maven/org.eclipse.angus/logging-mailhandler/pom.xml
MD5: d4925a2ff344f2fab35fdf31f4813b43
SHA1: 53aac2712cc43a3aed66f65536fd91709056aef1
SHA256:869577c24e1abb117bd9cf7dc9228c2643839b75087bfc5d6fed0d328ed9d1f7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	pom	artifactid	logging-mailhandler	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Mail logging handler	High
Vendor	pom	parent-artifactid	all	Low
Product	pom	artifactid	logging-mailhandler	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Mail logging handler	High
Product	pom	parent-artifactid	all	Medium
Version	pom	version	2.0.5	Highest

Identifiers

- pkg:maven/org.eclipse.angus/logging-mailhandler@2.0.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

mail.zip: angus-mail.jar (shaded: org.eclipse.angus:pop3:2.0.5)

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-mail.jar/META-INF/maven/org.eclipse.angus

/pop3/pom.xml
MD5: 0d7646a22486f0de9392d7ea120ff618
SHA1: 4b674f85989e5cc112b93427ec3852ef90359ba3
SHA256:64b065cc6bec31a1e5fefa9bf47382045cf048d69a9820da4cecc85f34a77a69
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	pom	artifactid	pop3	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Mail pop3 provider	High
Vendor	pom	parent-artifactid	providers	Low
Product	pom	artifactid	pop3	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Mail pop3 provider	High
Product	pom	parent-artifactid	providers	Medium
Version	pom	version	2.0.5	Highest

Identifiers

- pkg:maven/org.eclipse.angus/pop3@2.0.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:* (*Confidence*:Low) suppress

mail.zip: angus-mail.jar (shaded: org.eclipse.angus:smtp:2.0.5)

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-mail.jar/META-INF/maven/org.eclipse.angus/smtp/pom.xml
MD5: b5281897cc205fa3c8f0a93b58d4ba31
SHA1: c4b330d66629d75d0df7c09739c7ab37ca834011
SHA256:14923a712a69fb1408452be22fe8e87aa57e45337f0b52ae289d2bbb3d016ec1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	pom	artifactid	smtp	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Mail smtp provider	High
Vendor	pom	parent-artifactid	providers	Low

Product	pom	artifactid	smtp	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Mail smtp provider	High
Product	pom	parent-artifactid	providers	Medium
Version	pom	version	2.0.5	Highest

Identifiers

- pkg:maven/org.eclipse.angus/smtp@2.0.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:* (*Confidence*:Low) suppress

mail.zip: angus-mail.jar

Description:

Angus Mail Provider

License:

http://www.eclipse.org/legal/epl-2.0, https://www.gnu.org/software/classpath/license.html, http://www.eclipse.org/org/documents/edl-v10.php

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/angus-mail.jar
MD5: e965a2653568c0138457b4c6fc9e5d77
SHA1: 427f6d52ec0782f7efaca0c0732042e347a6cb4f
SHA256:b4d8c30d35f455def6c7a05fe595a1e62ea2b80cac3efec1e9ccf4118b23168a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	angus-mail	High
Vendor	jar	package name	angus	Highest
Vendor	jar	package name	eclipse	Highest
Vendor	jar	package name	mail	Highest
Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low
Vendor	Manifest	bundle-symbolicname	org.eclipse.angus.mail	Medium
Vendor	Manifest	provide-capability	osgi.serviceloader;osgi.serviceloader="jakarta.mail.util.StreamProvider",osgi.serviceloader;osgi.serviceloader="jakarta.mail.Provider"	Low

Vendor	pom	artifactid	angus-mail	Low
Vendor	pom	groupid	org.eclipse.angus	Highest
Vendor	pom	name	Angus Mail Provider	High
Vendor	pom	parent-artifactid	all	Low
Product	file	name	angus-mail	High
Product	jar	package name	angus	Highest
Product	jar	package name	eclipse	Highest
Product	jar	package name	mail	Highest
Product	jar	package name	util	Highest
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Angus Mail Provider	Medium
Product	Manifest	bundle-symbolicname	org.eclipse.angus.mail	Medium
Product	Manifest	provide-capability	osgi.serviceloader;osgi.serviceloader="jakarta.mail.util.StreamProvider",osgi.serviceloader;osgi.serviceloader="jakarta.mail.Provider"	Low
Product	pom	artifactid	angus-mail	Highest
Product	pom	groupid	org.eclipse.angus	Highest
Product	pom	name	Angus Mail Provider	High
Product	pom	parent-artifactid	all	Medium
Version	Manifest	Bundle-Version	2.0.5	High
Version	pom	version	2.0.5	Highest

Identifiers

- pkg:maven/org.eclipse.angus/angus-mail@2.0.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:angus_mail:2.0.5:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

mail.zip: bcjmail-fips.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/bcjmail-fips.jar
MD5: bed300b79a56bc057612f8a4cf97bba4
SHA1: 43ee8faa99aa5522da8a1895cafde67fd941478c
SHA256:2309e141a841c91db7dded3e6bc5d0666fbe5aee8443c8fece17b56f3d7b7dca
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bcjmail-fips	High
Vendor	jar	package name	bouncycastle	Highest
Vendor	jar	package name	bouncycastle	Low
Vendor	jar	package name	mail	Low
Vendor	jar	package name	smime	Low
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	application-name	Bouncy Castle FIPS JAKARTA S/MIME API	Medium
Vendor	Manifest	automatic-module-name	org.bouncycastle.fips.bcjmail	Medium
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Vendor	Manifest	bundle-symbolicname	bcjmail	Medium
Vendor	Manifest	caller-allowable-codebase	*	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	extension-name	org.bouncycastle.bcjmail.mail	Medium
Vendor	Manifest	Implementation-Vendor	BouncyCastle.org	High
Vendor	Manifest	Implementation-Vendor-Id	org.bouncycastle	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	BouncyCastle.org	Low
Vendor	Manifest	trusted-library	true	Low
Product	file	name	bcjmail-fips	High
Product	jar	package name	bouncycastle	Highest
Product	jar	package name	mail	Low
Product	jar	package name	smime	Low
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	application-name	Bouncy Castle FIPS JAKARTA S/MIME API	Medium
Product	Manifest	automatic-	org.bouncycastle.fips.bcjmail	Medium

		module-name		
Product	Manifest	Bundle-Name	bcjmail	Medium
Product	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Product	Manifest	bundle-symbolicname	bcjmail	Medium
Product	Manifest	caller-allowable-codebase	*	Low
Product	Manifest	codebase	*	Low
Product	Manifest	extension-name	org.bouncycastle.bcjmail.mail	Medium
Product	Manifest	multi-release	true	Low
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	trusted-library	true	Low
Version	Manifest	Bundle-Version	2.1.7	High
Version	Manifest	Implementation-Version	2.1.7	High

Identifiers

- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.7:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

mail.zip: bcpg-fips.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/bcpg-fips.jar
MD5: 11c7f0a1b7e012a2b9338c3a4942a447
SHA1: ad57be509cd778b05f92ff30f6758fb37adc51c5
SHA256:281ac18ecb0989b669847944da4cd0d89b40f83c294eb8b77dce1bcd2c707f3e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	bcpg-fips	High
Vendor	jar	package name	bcpg	Highest
Vendor	jar	package name	bouncycastle	Highest
Vendor	jar	package name	bouncycastle	Low
Vendor	jar	package name	openpgp	Highest

Vendor	jar	package name	openpgp	Low
Vendor	Manifest	application-library-allowable-codebase	*	Low
Vendor	Manifest	application-name	Bouncy Castle FIPS OpenPGP API	Medium
Vendor	Manifest	automatic-module-name	org.bouncycastle.fips.pg	Medium
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Vendor	Manifest	bundle-symbolicname	bcpg	Medium
Vendor	Manifest	caller-allowable-codebase	*	Low
Vendor	Manifest	codebase	*	Low
Vendor	Manifest	extension-name	org.bouncycastle.bcfips.pg	Medium
Vendor	Manifest	Implementation-Vendor	BouncyCastle.org	High
Vendor	Manifest	Implementation-Vendor-Id	org.bouncycastle	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	permissions	all-permissions	Low
Vendor	Manifest	specification-vendor	BouncyCastle.org	Low
Vendor	Manifest	trusted-library	true	Low
Product	file	name	bcpg-fips	High
Product	jar	package name	bcpg	Highest
Product	jar	package name	bouncycastle	Highest
Product	jar	package name	openpgp	Highest
Product	jar	package name	openpgp	Low
Product	Manifest	application-library-allowable-codebase	*	Low
Product	Manifest	application-name	Bouncy Castle FIPS OpenPGP API	Medium
Product	Manifest	automatic-module-name	org.bouncycastle.fips.pg	Medium
Product	Manifest	Bundle-Name	bcpg	Medium
Product	Manifest	bundle-requiredexecution	JavaSE-1.8	Low
Product	Manifest	bundle-symbolicname	bcpg	Medium

Product	Manifest	caller-allowable-codebase	*	Low
Product	Manifest	codebase	*	Low
Product	Manifest	extension-name	org.bouncycastle.bcfips.pg	Medium
Product	Manifest	multi-release	true	Low
Product	Manifest	permissions	all-permissions	Low
Product	Manifest	trusted-library	true	Low
Version	Manifest	Bundle-Version	2.1.13	High
Version	Manifest	Implementation-Version	2.1.13	High

Identifiers

- cpe:2.3:a:bouncycastle:bcpg-fips:2.1.13:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:2.1.13:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:openpgp:openpgp:2.1.13:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

mail.zip: jakarta.activation-api.jar

Description:

Specification

License:

EDL 1.0: http://www.eclipse.org/org/documents/edl-v10.php

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/jakarta.activation-api.jar
MD5: bc1602eee7bc61a0b86f14bbbb0cc794
SHA1: 9e5c2a0d75dde71a0bedc4dbdbe47b78a5dc50f8
SHA256:c9db52100ce6c8aac95cc39075f95720d2e561b11f8051b81c121ad4effd7004
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jakarta.activation-api	High
Vendor	jar	package name	activation	Highest
Vendor	jar	package name	jakarta	Highest
Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low

Vendor	Manifest	bundle-symbolicname	jakarta.activation-api	Medium
Vendor	Manifest	extension-name	jakarta.activation	Medium
Vendor	Manifest	implementation-build-id	3dad341	Low
Vendor	Manifest	Implementation-Vendor	Eclipse Foundation	High
Vendor	Manifest	specification-vendor	Eclipse Foundation	Low
Vendor	pom	artifactid	jakarta.activation-api	Low
Vendor	pom	developer email	bill.shannon@oracle.com	Low
Vendor	pom	developer id	shannon	Medium
Vendor	pom	developer name	Bill Shannon	Medium
Vendor	pom	developer org	Oracle	Medium
Vendor	pom	groupid	jakarta.activation	Highest
Vendor	pom	name	Jakarta Activation API	High
Vendor	pom	parent-artifactid	project	Low
Vendor	pom	parent-groupid	org.eclipse.ee4j	Medium
Vendor	pom	url	jakartaee/jaf-api	Highest
Vendor	pom (hint)	developer org	sun	Medium
Product	file	name	jakarta.activation-api	High
Product	jar	package name	activation	Highest
Product	jar	package name	jakarta	Highest
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Jakarta Activation API	Medium
Product	Manifest	bundle-symbolicname	jakarta.activation-api	Medium
Product	Manifest	extension-name	jakarta.activation	Medium
Product	Manifest	implementation-build-id	3dad341	Low
Product	Manifest	Implementation-Title	Jakarta Activation API	High
Product	Manifest	specification-title	Jakarta Activation Specification	Medium
Product	pom	artifactid	jakarta.activation-api	Highest
Product	pom	developer email	bill.shannon@oracle.com	Low
Product	pom	developer id	shannon	Low
Product	pom	developer name	Bill Shannon	Low
Product	pom	developer org	Oracle	Low

Product	pom	groupid	jakarta.activation	Highest
Product	pom	name	Jakarta Activation API	High
Product	pom	parent-artifactid	project	Medium
Product	pom	parent-groupid	org.eclipse.ee4j	Medium
Product	pom	url	jakartaee/jaf-api	High
Version	Manifest	Bundle-Version	2.1.4	High
Version	pom	parent-version	2.1.4	Low
Version	pom	version	2.1.4	Highest

Identifiers

- pkg:maven/jakarta.activation/jakarta.activation-api@2.1.4 (*Confidence*:High)

mail.zip: jakarta.mail-api.jar

Description:

Specification API

License:

EPL 2.0: http://www.eclipse.org/legal/epl-2.0
GPL2 w/ CPE: https://www.gnu.org/software/classpath/license.html
EDL 1.0: http://www.eclipse.org/org/documents/edl-v10.php

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/jakarta.mail-api.jar
MD5: a1872951f46b87594806bb01e342a468
SHA1: be9b3b677ed6083f575c437ebc442a6a4bd2b931
SHA256:aa493753acb7a8c45ba8f4c9cf1230a74e20237056dd5b5c8bc86c583e8cfa0e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jakarta.mail-api	High
Vendor	jar	package name	jakarta	Highest
Vendor	jar	package name	mail	Highest
Vendor	Manifest	bundle-docurl	https://www.eclipse.org	Low
Vendor	Manifest	bundle-symbolicname	jakarta.mail-api	Medium
Vendor	Manifest	extension-name	jakarta.mail	Medium
Vendor	Manifest	implementation-	e187321	Low

		build-id		
Vendor	Manifest	Implementation-Vendor	Eclipse Foundation	High
Vendor	Manifest	specification-vendor	Eclipse Foundation	Low
Vendor	pom	artifactid	jakarta.mail-api	Low
Vendor	pom	groupid	jakarta.mail	Highest
Vendor	pom	name	Jakarta Mail API	High
Vendor	pom	parent-artifactid	project	Low
Vendor	pom	parent-groupid	org.eclipse.ee4j	Medium
Product	file	name	jakarta.mail-api	High
Product	jar	package name	jakarta	Highest
Product	jar	package name	mail	Highest
Product	Manifest	bundle-docurl	https://www.eclipse.org	Low
Product	Manifest	Bundle-Name	Jakarta Mail API	Medium
Product	Manifest	bundle-symbolicname	jakarta.mail-api	Medium
Product	Manifest	extension-name	jakarta.mail	Medium
Product	Manifest	implementation-build-id	e187321	Low
Product	Manifest	Implementation-Title	Jakarta Mail API	High
Product	Manifest	specification-title	Jakarta Mail Specification	Medium
Product	pom	artifactid	jakarta.mail-api	Highest
Product	pom	groupid	jakarta.mail	Highest
Product	pom	name	Jakarta Mail API	High
Product	pom	parent-artifactid	project	Medium
Product	pom	parent-groupid	org.eclipse.ee4j	Medium
Version	Manifest	Bundle-Version	2.1.5	High
Version	pom	parent-version	2.1.5	Low
Version	pom	version	2.1.5	Highest

Identifiers

- pkg:maven/jakarta.mail/jakarta.mail-api@2.1.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:jakarta_mail:2.1.5:*:*:*:*:*:*:* (*Confidence*:High) suppress

mail.zip: mail.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/mail.jar
MD5: 947fa8f1ddc3bedd062e39f5b9a29811
SHA1: 9c0ae19820c2ca7688c7e2dfc1c420513b231820
SHA256:0c25c8fa33948103f08d32626d141f8b4b92ae12ce3e7d6e34434dd762f4c03b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	mail	High
Vendor	jar	package name	api	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	mail	Low
Vendor	Manifest	built-date	2026-09-28 17:42	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	mail	High
Product	jar	package name	api	Low
Product	jar	package name	mail	Highest
Product	jar	package name	mail	Low
Product	jar	package name	shared	Highest
Product	Manifest	built-date	2026-09-28 17:42	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	mail	High
Product	Manifest	specification-title	mail	Medium
Version	jar	package name	shared	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

mail.zip: mail.jar: smimeconfig.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/mail.zip/mail.jar/com/inet/mail/structure/smimeconfig.js
MD5: 5bcf984b6f7d3c12903f8e45723c4737
SHA1: c0fefbb10badfba57b9dd391e641c1357c10b615
SHA256:0fd57f5869585f955a1274b3e859d7172f1d8c41f26fb647d256207d680c5567
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance-javadoc.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar
MD5: e89ac87bbebfe2c6c831fc9b249041ec
SHA1: a8442a5e37090be7dc06587dd037f6ccde4f210e
SHA256:6d55676bb83ef074aadde7c4b890083274809e29d67fe019762df3fa8c14b00a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	maintenance-javadoc	High
Product	file	name	maintenance-javadoc	High

Identifiers

- **None**

maintenance.zip: maintenance-javadoc.jar: member-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/member-search-index.js
MD5: d2f21acbf71acf3041122496263b6987
SHA1: 84b4c22fabbd5df572518bbccbbdb96b3936b6fc
SHA256:dd41c917e08c1e6b0b4cac7e70d4284187f4c49eb8e3d6f4c208031b21e5291a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance-javadoc.jar: package-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/package-search-index.js
MD5: 855175baa750c5c598744cead48c703b
SHA1: 0c42882b706bfb4b9e6395f33e47c199af9ad99c
SHA256:2fedad883e306a57bd45bc9d379ebaf73e07a74f40b222a6bd6636a128e02321
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance-javadoc.jar: tag-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/tag-search-index.js
MD5: a58a1c5776c62196a0f461efeec112cf
SHA1: 1f0fdbb7c073f10c3554bd94ad9a08e02540e79d
SHA256:c152193c680dff2fca6c2f8feec029f8a15b07527def9ddcd88eb0a078c5e704
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance-javadoc.jar: type-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance-javadoc.jar/type-search-index.js
MD5: 5f0f0ccdd4505d0bec8b945166307218
SHA1: 5595ef71303f817751c27596da180e8e8866f2b4
SHA256:25da93efbedae785d430a8c419d14ea9bb9e1eef9d948f36e27ee8ce803392be
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar
MD5: f6cd702862b215a9cdef9f66082a9bd2
SHA1: 05d8f73ba1143762f20f9cb0433e095ae951236c
SHA256:0fcafe28e41849e8a3729920b44a86103f4b9d2df21bf4e7938ebf035cbc6080
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	maintenance	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	maintenance	Low
Vendor	jar	package name	server	Low
Vendor	Manifest	built-date	2026-09-28 17:23	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	maintenance	High
Product	jar	package name	maintenance	Highest
Product	jar	package name	maintenance	Low
Product	jar	package name	server	Low
Product	Manifest	built-date	2026-09-28 17:23	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	maintenance	High
Product	Manifest	specification-title	maintenance	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

maintenance.zip: maintenance.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance

/resources/backup/js/controller.js
MD5: fe6818816e978228640f9daccd5fa648
SHA1: c92e91447b09b4ae9d35835ae100e2b923e41a1c
SHA256:04277068764a3a193a96bc2c5ce6ae2fb96ce5d81eec2a3153fe96ab3e7a81ea
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/resources/cache/js/controller.js
MD5: 9aed8a6ed9f9e734d77c32d719bec6c3
SHA1: f1e50c3fe93c975c1900d7bb2f6e3903805466a8
SHA256:153239e343c82ae0a4a573dfcfd0292c52b77816297b77830d59aea2dd2c5c6a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/resources/main/js/controller.js
MD5: 0ff72e191a3f127973fc5a9381f1e3fb
SHA1: 2ed064d4500a047ef82b23173f0abf1e9813e1a2
SHA256:6d60b6004b5b228cc1e6fcaf6ba01afc922d7d6e174f32773dbf32f1993085a0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/resources/programdata/js/controller.js
MD5: fa453d5635f82f0078c224f27dd99a7d
SHA1: 6288a3c4fbff29ee7cc6a8f69149de44c49ef5c6
SHA256:f7902fb5b8dd900a95b90969872c55787e2d4f65f3736d827fcb13c0ebcef46b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/resources/usercleanup/js/controller.js
MD5: 8761a32cdcf4e1e4a7685026230292f7
SHA1: c2d0abdc930a08da61c93cf63f310c9a74434f3c
SHA256:358479a73183963c1626c72ae92d5c4f7c03b83363c80257ac03dc58eb4285bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: filechooser.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/resources/main/js/filechooser.js
MD5: e68e2ea53d15557b2fb1deaf06d441d3
SHA1: 047d5f2582143536ea470e92aa91fb7b77c7f093
SHA256:c44d53718171530ce586b9932fe7126a09de8e6f7bb9e40aaf949483e432e87d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: loginmodification.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/server/loginmodification/js/loginmodification.js
MD5: c9caaf80af602574445f7bd08806acb4
SHA1: 95812b03c104f2a6adfbbf273a0218e2d70f52da
SHA256:145a041432ca0a48250e35f28ce0aaba8b9d33a0b5868d9a580bbb75ae2446bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

maintenance.zip: maintenance.jar: multieditusers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/maintenance.zip/maintenance.jar/com/inet/maintenance/resources/usercleanup/js/multieditusers.js
MD5: 9344849a6f020a58c0f0d718e8c76929
SHA1: 2d636915befebb9bd1db90c54bffe6acfb088d87
SHA256:ab73fb84fe0687eaea50fa310992eb630da346b49387ccee829854f6ecc03329
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

mongodb-driver-core.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/persistence/mongodb-driver-core.jar
MD5: 264243de63a928ff1a599f4e7cb7c79a
SHA1: c2b86ff256c0fb0f2e5763d0872a69d099210e3c
SHA256:b83a6c1a2b98c485ecbffa442b2c13bd6c080be91ea1c1da320ff257df0918a7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	mongodb-driver-core	High
Vendor	jar	package name	internal	Low
Vendor	jar	package name	mongodb	Highest
Vendor	jar	package name	mongodb	Low
Vendor	Manifest	automatic-module-name	org.mongodb.driver.core	Medium
Vendor	Manifest	bundle-symbolicname	org.mongodb.driver-core	Medium
Product	file	name	mongodb-driver-core	High
Product	jar	package name	internal	Low
Product	jar	package name	mongodb	Highest
Product	Manifest	automatic-module-name	org.mongodb.driver.core	Medium

Product	Manifest	Bundle-Name	mongodb-driver-core	Medium
Product	Manifest	bundle-symbolicname	org.mongodb.driver-core	Medium
Version	Manifest	build-version	5.9.2	Medium
Version	Manifest	Bundle-Version	5.9.2	High

Identifiers

- **None**

mongodb-driver-sync.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/persistence/mongodb-driver-sync.jar
MD5: 5caf93339ced7aea4134d2a931027875
SHA1: 9d88572cb265d86175181b260fe855f8c72161aa
SHA256:a47d2f52284e2f6053b4047b3036d42f25a53a7f6151a7f9d87eaa887776f095
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	mongodb-driver-sync	High
Vendor	jar	package name	client	Highest
Vendor	jar	package name	client	Low
Vendor	jar	package name	internal	Low
Vendor	jar	package name	mongodb	Highest
Vendor	jar	package name	mongodb	Low
Vendor	Manifest	automatic-module-name	org.mongodb.driver.sync.client	Medium
Vendor	Manifest	bundle-symbolicname	org.mongodb.driver-sync	Medium
Product	file	name	mongodb-driver-sync	High
Product	jar	package name	client	Highest
Product	jar	package name	client	Low
Product	jar	package name	internal	Low
Product	jar	package name	mongodb	Highest
Product	Manifest	automatic-module-name	org.mongodb.driver.sync.client	Medium

Product	Manifest	Bundle-Name	mongodb-driver-sync	Medium
Product	Manifest	bundle-symbolicname	org.mongodb.driver-sync	Medium
Version	Manifest	build-version	5.9.2	Medium
Version	Manifest	Bundle-Version	5.9.2	High

Identifiers

- **None**

notification.zip: notification.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/notification.zip/notification.jar
MD5: df3468c20520c38cb9c1b08c0dffe5f1
SHA1: 7f9e27e8c45fb78b4d184d0911b302e4cc5ad6fd
SHA256:50528ca03e1ca9a26f77143f17c8f222a1d6970edf5c9a5c97c39c655db63b80
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	notification	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	notificationui	Low
Vendor	jar	package name	server	Low
Vendor	Manifest	built-date	2026-09-28 17:38	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	notification	High
Product	jar	package name	notificationui	Low
Product	jar	package name	server	Low
Product	Manifest	built-date	2026-09-28 17:38	Low

Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	notification	High
Product	Manifest	specification-title	notification	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

notification.zip: notification.jar: notification.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/notification.zip/notification.jar/com/inet/notificationui/client/js/notification.js
MD5: dda8e15da399d47bdb72f73795677a94
SHA1: 79a02965f4b39dfd2cdc5ccd14c712d98315aabd
SHA256:8a4e082c22d82b55e9c85ac6dbe5fd08570e3fc97c51d8ccee3fe9f17267ee2f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

notification.zip: notification.jar: notification_config.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/notification.zip/notification.jar/com/inet/notificationui/client/js/notification_config.js
MD5: 323c074408d9e2dc2145230f2f2bec9e
SHA1: e6ca6eb13f3c22aedfbd90b0d7306c35cd7d2b28
SHA256:c86eed2c4c6b7df65bdebffc00a3ea2d809997c4b7a97cd22d55f7193ebd4b94
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

notification.zip: notification.jar: notification_taskplanner.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/notification.zip/notification.jar/com/inet/notificationui/client/js/notification_taskplanner.js
MD5: 15154b69fa215362e2ff26d2aa4e4c86
SHA1: 71f34cbc1808feecc0f1478dbb859a51528c7924
SHA256:a668b0da62af928ee49b974a4d024017e0c583736274bc83170689afb4417b24
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

notification.zip: notification.jar: targetrenderer.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/notification.zip/notification.jar/com/inet/notificationui/client/js/targetrenderer.js
MD5: 9207efb9b92d4108c031b3e7f469ccff
SHA1: fc19cd09c51417a29979d39e3a74a2d99fbf9c03
SHA256:c6c83159f063f74a44c1d68bd67a67c4c96023c3eba9f87ce1090b8f994f49bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

opentest4j-1.3.0.jar

Description:

Open Test Alliance for the JVM

License:

The Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.opentest4j/opentest4j/1.3.0/152ea56b3a72f655d4fd677fc0ef2596c3dd5e6e/opentest4j-1.3.0.jar
MD5: 03c404f727531f3fd3b4c73997899327
SHA1: 152ea56b3a72f655d4fd677fc0ef2596c3dd5e6e
SHA256:48e2df636cab6563ced64dcdff8abb2355627cb236ef0bf37598682ddf742f1b
Referenced In Project/Scope: CoWorkInstaller:inetPlugin
Included by:

- pkg:maven/org.junit.jupiter/junit-jupiter-engine@6.1.3
- pkg:maven/org.junit.jupiter/junit-jupiter@6.1.3
- pkg:maven/org.junit.platform/junit-platform-suite@6.1.3

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	opentest4j	High
Vendor	gradle	artifactid	opentest4j	Highest
Vendor	gradle	groupid	org.opentest4j	Highest
Vendor	jar	package name	opentest4j	Highest
Vendor	jar	package name	opentest4j	Low
Vendor	Manifest	build-date	2023-07-06	Low
Vendor	Manifest	build-revision	214973bfa4e7e9be7d04e623202cc4147c7036	Low
Vendor	Manifest	build-time	14:25:06.116+0200	Low
Vendor	Manifest	bundle-symbolicname	org.opentest4j	Medium
Vendor	Manifest	Implementation-Vendor	opentest4j.org	High
Vendor	Manifest	specification-vendor	opentest4j.org	Low
Vendor	pom	artifactid	opentest4j	Low
Vendor	pom	developer email	business@johanneslink.net	Low
Vendor	pom	developer email	mail@marcphilipp.de	Low
Vendor	pom	developer email	matthias.merdes@heidelpay.com	Low

Vendor	pom	developer email	sam@sambrannen.com	Low
Vendor	pom	developer email	stefan.bechtold@me.com	Low
Vendor	pom	developer id	bechte	Medium
Vendor	pom	developer id	jlink	Medium
Vendor	pom	developer id	marcphilipp	Medium
Vendor	pom	developer id	mmerdes	Medium
Vendor	pom	developer id	sbrannen	Medium
Vendor	pom	developer name	Johannes Link	Medium
Vendor	pom	developer name	Marc Philipp	Medium
Vendor	pom	developer name	Matthias Merdes	Medium
Vendor	pom	developer name	Sam Brannen	Medium
Vendor	pom	developer name	Stefan Bechtold	Medium
Vendor	pom	groupid	org.opentest4j	Highest
Vendor	pom	name	org.opentest4j:opentest4j	High
Vendor	pom	url	ota4j-team/opentest4j	Highest
Product	file	name	opentest4j	High
Product	gradle	artifactid	opentest4j	Highest
Product	jar	package name	opentest4j	Highest
Product	Manifest	build-date	2023-07-06	Low
Product	Manifest	build-revision	214973bfa4e7e9be7d04e623202cc4147c7036	Low
Product	Manifest	build-time	14:25:06.116+0200	Low
Product	Manifest	Bundle-Name	opentest4j	Medium
Product	Manifest	bundle-symbolicname	org.opentest4j	Medium
Product	Manifest	Implementation-Title	opentest4j	High
Product	Manifest	specification-title	opentest4j	Medium
Product	pom	artifactid	opentest4j	Highest
Product	pom	developer email	business@johanneslink.net	Low
Product	pom	developer email	mail@marcphilipp.de	Low
Product	pom	developer email	matthias.merdes@heidelpay.com	Low
Product	pom	developer email	sam@sambrannen.com	Low
Product	pom	developer email	stefan.bechtold@me.com	Low
Product	pom	developer id	bechte	Low
Product	pom	developer id	jlink	Low
Product	pom	developer id	marcphilipp	Low

Product	pom	developer id	mmerdes	Low
Product	pom	developer id	sbrannen	Low
Product	pom	developer name	Johannes Link	Low
Product	pom	developer name	Marc Philipp	Low
Product	pom	developer name	Matthias Merdes	Low
Product	pom	developer name	Sam Brannen	Low
Product	pom	developer name	Stefan Bechtold	Low
Product	pom	groupid	org.opentest4j	Highest
Product	pom	name	org.opentest4j:opentest4j	High
Product	pom	url	ota4j-team/opentest4j	High
Version	file	version	1.3.0	High
Version	gradle	version	1.3.0	Highest
Version	Manifest	Bundle-Version	1.3.0	High
Version	Manifest	Implementation-Version	1.3.0	High
Version	pom	version	1.3.0	Highest

Identifiers

- pkg:maven/org.opentest4j/opentest4j@1.3.0 (*Confidence*:High)

persistence.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/persistence/persistence.jar
MD5: 09209ab35beb76719e0b204a47232dd9
SHA1: c148ae425623e75cc21ab2975f200b5f42e14bc9
SHA256:890e7578d30b4983f598fa76801babaea276d1b9a2ec0b48699f9ef6ecff6dfa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	persistence	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	persistence	Low
Vendor	Manifest	built-date	2026-09-28 17:29	Low
Vendor	Manifest	implementation-	shared	Low

		group		
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	persistence	High
Product	jar	package name	persistence	Highest
Product	jar	package name	persistence	Low
Product	Manifest	built-date	2026-09-28 17:29	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	persistence	High
Product	Manifest	specification-title	persistence	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar
MD5: 9ed390f786a17da08cabcc261991bd1f
SHA1: f619bebdd6b4c9285129cc75b6975d64b9babecc
SHA256:1e7b50e4b3fbed15ce87b5e6ff897d5084ff97be6a64f589a7c80177d3e2eb0d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	pluginstore.client	High
Vendor	jar	package name	client	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	store	Low

Vendor	Manifest	built-date	2026-09-28 17:43	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	pluginstore.client	High
Product	jar	package name	client	Highest
Product	jar	package name	client	Low
Product	jar	package name	shared	Highest
Product	jar	package name	store	Low
Product	Manifest	built-date	2026-09-28 17:43	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	pluginstore.client	High
Product	Manifest	specification-title	pluginstore.client	Medium
Version	jar	package name	shared	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar/com/inet/store/client/setup/controller.js
MD5: b890353af95e8d67ed666d72e55d5583
SHA1: cdc7ae95f6ea08ce7051388a5a6487c8a965eec3
SHA256:b2efe42a4dfe713e2a079e24a1044fdc777effb0518d6750fdf9a3974ac78936
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar: pluginstorehelpcontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar/com/inet/store/client/plugin/help/js/pluginstorehelpcontroller.js
MD5: 33e0b25623e005ecbba43c00c91b043a
SHA1: 6b9855a487458ce85ae48ee1c5a129b26093b289
SHA256:a70a95787e2759bf1d43b76947ea5d48e541c6d94c640d25c9efd31ce281e3a7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar: publicstoreconfig.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar/com/inet/store/client/ui/js/publicstoreconfig.js
MD5: 640b897e30bb04f24b310e948f963701
SHA1: c4f24830c5130eabd110ac29f1e198ca4f88e35b
SHA256:45bf77256d46306542a6592243af524e1be940c5bef8746be0fd62ec7209eb84
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar: storecontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar/com/inet/store/client/ui/js/storecontroller.js
MD5: 512668a61bc16fe85f6442a56f622a9d
SHA1: f9bc6cb342455404802657a7c0d1dd1ed6ec7297
SHA256:7f183982c67d73d4a2bfb963dcc5aa8241b3beb2f2acf5d19aaec20357b715d6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar: storedirectives.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar/com/inet/store/client/ui/js/storedirectives.js
MD5: ec0e5529e70952af58b9df0ce2bfebb4
SHA1: 0b859497e1b59e55936959192636c3fec9bacef5
SHA256:5066f9af1ecc472186f35289ec17fd270e6a0ef404796f1fbe6acdf69c40fe90
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

pluginstore.client.zip: pluginstore.client.jar: storemodel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/pluginstore.client.zip/pluginstore.client.jar/com/inet/store/client/ui/js/storemodel.js
MD5: 79df37a017eb872811c499812d1eb6dc
SHA1: 1765bf02e7673e3559cac97d4e8a8308c3cf7fcb
SHA256:763d9661e237f8406a59f8fbec70549b5f4cf3e70e58b0c038bc233447d29669
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular-animate.jar

Description:

WebJar for angular-animate

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar
MD5: 1dcc988a8392618e7c5127f57b3453d1
SHA1: 7ea94213dad8a46ab088e1a3dd6a5def2ecf8e78
SHA256:dbbce06145963ef7bfd197c1646722fedfe76a9b54b01f1b6dc7ccf7e8b51163
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	angular-animate	High
Vendor	pom	artifactid	angular-animate	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	angular-animate	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	angular-animate	High
Product	pom	artifactid	angular-animate	Highest

Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	angular-animate	High
Product	pom	url	https://www.webjars.org	Medium
Version	pom	version	1.8.3	Highest

Identifiers

- pkg:maven/org.webjars.npm/angular-animate@1.8.3 (*Confidence*:High)

remotegui.zip: angular-animate.jar: angular-animate.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.js
MD5: 31312b87e7226c8bf0714fcef0ea5d18
SHA1: dc9fb55f2c7f922c5ba83449266239ba1353db45
SHA256:58e79e0e7cbb1e1502d216701e1fae41c405d92320aea1b68a223054096fda93
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular-animate.jar: angular-animate.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.min.js
MD5: 5d2d0f42bb7e1b5503e914674f59dad0

SHA1: 4c15a58541e53c451c6f946d2048104f88b833c7
SHA256:8e6202b1330a469a61ccdeebbd1cb3a20d0ecdfc8d106f68da5b85e9b67a1cd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular-animate.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/index.js
MD5: eca59ea32960ae595dd18ad9480185b1
SHA1: b8fe1c0a06b723a75c7e596fd8a86d91965f681c
SHA256:7f2f9350e5624bf86e8760d1deae03fae4477949284b49471eb67e2b6498cb7d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular-animate.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/package.json
MD5: 13957f0482b591f50a2e9528a5b84330

SHA1: 16ec0d9e9e70f179261a1bd672e610b159876ff5
SHA256:e2fcbc9996d890ec0c6601b2c9176a1ada7806e1dcd6eca8549bba9022235877
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular-cookies.jar

Description:

WebJar for angular-cookies

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar
MD5: 5d743cd15e44b5a942478abaa3a008ae
SHA1: 2ebe196f9032e261a470467b5a14632d81d3d4f9
SHA256:0809dd125183f03e6682985208de5f1221478221ed41667545133f7e729dd000
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	angular-cookies	High
Vendor	pom	artifactid	angular-cookies	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	angular-cookies	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	angular-cookies	High
Product	pom	artifactid	angular-cookies	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	angular-cookies	High

Product	pom	url	https://www.webjars.org	Medium
Version	pom	version	1.8.3	Highest

Identifiers

- pkg:maven/org.webjars.npm/angular-cookies@1.8.3 (*Confidence*:High)

remotegui.zip: angular-cookies.jar: angular-cookies.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/angular-cookies.js
MD5: e17187aea1f0e6dbd25722e34b754915
SHA1: 20f43f716b9fef7d72537bc1b0e5aa2bc480cee5
SHA256:f3291c552042f6d0c500167769912a78ab3ecec9917128b2d6ea8e7c6714bb97
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular-cookies.jar: angular-cookies.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/angular-cookies.min.js
MD5: c41aff8423276d46f0d02de6dcb71524
SHA1: 7dc53f75d5bf7dd2c770cb50f31242c70193c086
SHA256:926509b494009bea03288bba191a2b238032188e9112377e50fbfe7814c6639b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular-cookies.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/index.js
MD5: 88188b8869bb0cbae63eb86aa6c1059a
SHA1: ce388b565b0d0392802138b2a7d4bf393c3d49f9
SHA256:b1b8d54ed8400d4f997da0f2fa672e8728d4771a77028d9f495cf1732fcb1e6f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular-cookies.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/package.json
MD5: 6785fbb341602e147af808078db0d42b
SHA1: a30ac55dae62b1a7c8921c7687a3276dbeeed564
SHA256:81847196d700fe42834ebf82cb0c68267d9c237134566556a466e070659c7222
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular-sanitize.jar

Description:

WebJar for angular-sanitize

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar
MD5: f47ca0f7e843acea25d245b34ce30feb
SHA1: 8050e163f66fb899645cc67ffa67d92a25096902
SHA256:4de072c9e746b2bf70aee70cc1c9b61350e017002dd71089e5f66a587f7ed92f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	angular-sanitize	High
Vendor	pom	artifactid	angular-sanitize	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	angular-sanitize	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	angular-sanitize	High
Product	pom	artifactid	angular-sanitize	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	angular-sanitize	High
Product	pom	url	https://www.webjars.org	Medium
Version	pom	version	1.8.3	Highest

Identifiers

- pkg:maven/org.webjars.npm/angular-sanitize@1.8.3 (*Confidence*:High)

remotegui.zip: angular-sanitize.jar: angular-sanitize.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/angular-sanitize.js
MD5: 0127d7a139abfc8bd45875a9c8ea6348
SHA1: 197aea2acc25a0fa821766400950cac58a3627a5
SHA256:c84c65250afe5a1265f36a7e16c6010652e55c2ae3a779c351fb68536c42bf64
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular-sanitize.jar: angular-sanitize.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/angular-sanitize.min.js
MD5: f3c62abeec216e9431e7d5b22d8e813b
SHA1: 21355ef18c5e1ce2b2c711b9dba21cbea0655646
SHA256:cc80a30ad0439c2e9c209b3d7fcffb1d10e6007fd1d00c9cc144f393664a7045
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular-sanitize.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/index.js
MD5: 796078246b8e97f002ea5c97c4c7de54
SHA1: 0ce03000a4c04ae0a8b4353715bda54b8a8e8c69
SHA256:44cbd8c36c3e2818d011eb0dc7d95293730667fa5a98a23449e9b4add369f65b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular-sanitize.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/package.json
MD5: 515d23261280a10a4d84ed267c425880
SHA1: 84d37bbaefc2117ac59c79b0d87a953a1abd4911
SHA256:5e5c191e41b4e9902cfaeb95878d5b92333585e6dad936588fe1adfd1445af86
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular.jar

Description:

WebJar for angular

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar
MD5: f339a9a66a64c67eebb21ec3b251dfc6
SHA1: cff4aee339a9ca4ae2f095079930edeaad6a94ee
SHA256:a997eb40987ddb5d3bf64adf3d33afcff3ac2b1eb2e7255b5203a387f8097cd0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	angular	High
Vendor	pom	artifactid	angular	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	angular	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	angular	High
Product	pom	artifactid	angular	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	angular	High
Product	pom	url	https://www.webjars.org	Medium
Version	pom	version	1.8.3	Highest

Identifiers

- pkg:maven/org.webjars.npm/angular@1.8.3 (*Confidence*:High)

remotegui.zip: angular.jar: angular.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.js
MD5: e09f650a016c24bc1b5a1edc93bfbade
SHA1: 0f1f7445b761b9bbd5385f9f0b316dbf1ca48696
SHA256:fdca889e76f55fdee7ab661920f37ce19233563bf7f4ac8120f8ebc2ac768768
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular.jar: angular.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.min.js
MD5: 967a32633fa8f38f4ac3376c1a37b992
SHA1: b53b74d8e0b732dcdb98fbe521146b88299ea2f1
SHA256:396dc1a03d6cc02e9c51a80246e0db53c5c8df9bd07287e3b51bce4a29dab355
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Identifiers

- pkg:javascript/angularjs@1.8.3 (*Confidence*:Highest)

remotegui.zip: angular.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/index.js
MD5: 0d848853205d22ab8be985876aec948a
SHA1: a2bfe847bea879ad2775509c4421291c404d8c21
SHA256:d469f8e93a4c345f01d81d162a803116de1bc6afd4bfeba8b45951449956b686
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: angular.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/package.json
MD5: c5e0d73dc5121cf479c775248d2ca497
SHA1: bc29d1f7c080dfb1f701ad4f1c4ff548916f28e5
SHA256:95ad7872af90c37e7a5597581f5bb2362d59c49fc3f2766dd9f2568a041cf10a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar

Description:

WebJar for codemirror

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar
MD5: 489d39ab98876cdb012faabde1b3148f
SHA1: c8e1fd16401dc9ca22ca8cbc3552ee5f80111f50
SHA256:5d5bf6889f3eede1c9e1a551ce452d1c88de1444fa8125cbbbb6d301a730aa9b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	codemirror	High
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	org.webjars.npm.codemirror	Medium
Vendor	pom	artifactid	codemirror	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	codemirror	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	codemirror	High
Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	codemirror	Medium
Product	Manifest	bundle-symbolicname	org.webjars.npm.codemirror	Medium
Product	pom	artifactid	codemirror	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	codemirror	High
Product	pom	url	https://www.webjars.org	Medium
Version	Manifest	Bundle-Version	5.65.21	High
Version	pom	version	5.65.21	Highest

Identifiers

- pkg:maven/org.webjars.npm/codemirror@5.65.21 (*Confidence*:High)
- cpe:2.3:a:codemirror:codemirror:5.65.21:*:*:*:*:*:*:* (*Confidence*:High) suppress

remotegui.zip: codemirror.jar: CodeMirror.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/CodeMirror.js
MD5: d154477df9eebe156a1a493731acb01d
SHA1: 69efd74f28f36317a2bb9101dbbaec73f5ca3735
SHA256:258db73a89eb6d88475013d38f4e0e01cc1476788f931058bf470db1ee26ca53
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ContentEditableInput.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/ContentEditableInput.js
MD5: c413c67a304f44b5c6abe741d1375cf5
SHA1: f730eba73ed0035fc992d30233f7b3a83f39d903
SHA256:3aa3c7e07a9b5f85982f6b4d961364a105af1c902b072ee9514bfd52bb82ac40
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: Display.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/Display.js

MD5: 80c3c344a0449c4af2684549e142bdfe
SHA1: c20c918f71472f08bd42ee2eb8c6852da9a2f7b7
SHA256:5b590443c84aaf6575ebf62fb41f497e5a55f1b97166066463651ec905a8644f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: Doc.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/Doc.js
MD5: 66f02c635454d1ae55f7472709417566
SHA1: 8799d7becd0b3ee9bfd397c157c43ca6ebb264d0
SHA256:32bf377fa99365b49732f69c5e565c61995fefdf8d0bc6f3404d4fc00ed8ac7f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: StringStream.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/StringStream.js
MD5: d187f08909bf9bb188d04c79f089c26a
SHA1: f5c4fc956b8b4de762087204024eb625cb00a790
SHA256:9f1ab50bba4ae102fa5c611d4ef5b056d063a63a7f20cfef59eea64e93c3e04e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: TextareaInput.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/TextareaInput.js
MD5: 21a07808f1d702b19ec423489301c349
SHA1: ee003a81f700f183c31ced6597bffabd99ab8d54
SHA256:c08855459181c879b3da30d27702645dd2b34b1258b21636ef1e60dea33a9727
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: active-line.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/selection/active-line.js
MD5: 774e515fe054cbcd6cc869bfd550b17d
SHA1: 3d950f5055286088e93e0ee4c8a1d62eaf8aedac
SHA256:3afbcf78835c9bdc342e3992c53d9b74286722613bb1a8adc9d140edc8737ee8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: annotatescrollbar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/scroll/annotatescrollbar.js
MD5: a9dfd7f9d78bd36c617429ed88cb67e5
SHA1: ad1133e5432a7c65881747c87c84529fed297ecb
SHA256:9041e8d81e3cebc481cabfae90d3b80596f3194de75d98e5526d3bfa44ae3bbc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: anyword-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/anyword-hint.js
MD5: ba7fa17b24f0937d9431f93b9de2da37
SHA1: a87db7c6de5231a1bfd702e26ecf4aa76d822a0a
SHA256:e834ad178bd23449476e29179e8cb9f0c1ebaed35dab9059ed9a46b388271f3e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: apl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/apl/apl.js
MD5: c0d55e310ae0a4290d3fccca84bff448
SHA1: 006c98d2b17e85168065eebf44c3fdd91b9ff874
SHA256:47e0fdac0a39e0186019064e13b674dda4223b03b2748d34cccc09489fde2674
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: asciiarmor.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/asciiarmor/asciiarmor.js
MD5: 42e5c7f3f48fa085f63bd7708bb204fd
SHA1: b15cdadbf5a869d06a79e6a9e187d0509dca1239
SHA256:bdcb68c4b0c9dc53b2af587673461a495f123a5b9da8f6be79d97fee2790f9ae
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: asn.1.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/asn.1/asn.1.js
MD5: a928fdb102ef88113a9d1c0d9e520114
SHA1: f293930644bd6093dbb02475e8b409fe9794f437

SHA256:5b50cca4b34820cb3d57c218945ff2d870d57eba83e13c2c66590063e2a23acc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: asterisk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/asterisk/asterisk.js
MD5: 2f4e25e805d878f43b8568609c48dba8
SHA1: 109a76d631e43dd32c13cbb0c23ad83e1851ad0a
SHA256:0849e3a141e967559d752de2205956cb690f1d4ba0a5ace5481c6c565db9b674
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: autorefresh.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/display/autorefresh.js
MD5: 16b07faa9ef79a1fb79432fb4f4a9e3a
SHA1: 091a2b17758e7c3182542314256139a2247b508c
SHA256:2ec9d5585bd24d7611f30ebbb1cd8fedf79747cf89c1f83852dd1dd9981f10bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: bidi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/bidi.js
MD5: 22a12be2f1e24a9bfddc5c3b0d187ede
SHA1: ab735d3376e0040172b6dc972f97df663f231dc4
SHA256:0a4646d7a1214acfc71ad351d021f31795b056ce7a08f80d29857aeca1a5163b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: brace-fold.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/brace-fold.js
MD5: d56849bd7cce8a10ccb842d50f0de179
SHA1: 4103103f28436925442d5397c24425fbaf660fce
SHA256:2907087538a295e5b4f084f8c5ee7eba35cc973db194cbf596ab13a6c97a6834
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: brainfuck.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/brainfuck/brainfuck.js
MD5: f3ff733b3609dfb34a49652f6a4a2d09
SHA1: 41a8164ddba5e25fe2401265eb9fd4222e415549
SHA256:67496a83fe1ea3304a3f65a8f8196f3a4a40060ea4febcbb60a82c7657205abd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: browser.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/browser.js
MD5: 564eafde7c1566f1b9b0d976cc3ace2f
SHA1: 2c592606b3242ac9cf080d138aae3516cc2ef05d
SHA256:de647094595511fabe9d548d9e45dacf746d7b83a198cb69b5b8859fa3eccb30
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: change_measurement.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/change_measurement.js
MD5: 39707c0eb637648efc07d95bb60253d3
SHA1: 025a52f620cc5b6edee8fb9c63a3f6ecf4c2284c
SHA256:1d1648706bf317acc33a64673cb4fbc2d2a7db8205bcc1cd9fe52819c13b87f0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: changes.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/changes.js
MD5: 822465b81d600e9a703579605e2147bc
SHA1: 1b77f1034de1cac51a8ff50e48f9604bc62556e5
SHA256:13b0b2c417e0181ec9cb012932c1fa167c50171133391c00582e2939206362a0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: chunk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/chunk.js
MD5: 7dd1b45f75341b5a03a01f6607da69a4
SHA1: 89dfb21758e8a384033d09678a8d5b1ce8983e6f
SHA256:18f55da6b39c1b12fb5406c7962a88884e00d2122566622784720cbe612fc676
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: clike.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/clike/clike.js
MD5: 67fa856e3fde2a4527bd5dcd4fd905b8
SHA1: 4efa3324706224dbbb6ba8c5b574c413693e3935
SHA256:058a0a64a206b1e4dbcc19a6ffa4015a84bb6bfe13d0ba85768be11def5b4ed2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: clojure.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/clojure/clojure.js
MD5: e37bb512800e28450cd3f697c081dcf6
SHA1: d34f8c3b12f61b2238ce71c315a5dc9ca045b7ba
SHA256:c5f9d7d14b3037dc35b74a811dce7f7a81a02aa5e6fd9e2b67afc1a91948ca1e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: closebrackets.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/edit/closebrackets.js
MD5: 667059f346609f6ad778936b17c43824
SHA1: 248b45be826a8856a0ed0733c8511d9d0c595507
SHA256:143c3014c29254f3531cc30be6d90205084bcfc36cffa6f9b2a46fd42a40be20
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: closetag.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/edit/closetag.js
MD5: 744876ab906996c429eef7654278f514
SHA1: 0e0e10e59f93f87c9bc35247b14831091113adb4
SHA256:6fbe2b93cc1744d9e14ad1d613449f7e16df4c2aa2842f658efc17abf662f850
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: cmake.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/cmake/cmake.js
MD5: fc204bb5f2393f59bcd34a860f1e1a57
SHA1: 73985b80cdb80d12831a7476b740733e3fdd065d
SHA256:6379ded0f75af38659031d1eaa803d2bd5be0fa7cebc216e55ca65d01a35bf1a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: cobol.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/cobol/cobol.js
MD5: d8a271c0bf27ef5cc2dd8ea19886aa75
SHA1: 93072b3c895318fc58f8ed16d68cc213ac7910de
SHA256:0cecf82da2915c20187ab4e29cfc4abbb0078536874b27978726d48371487e4c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: codemirror-standalone.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars

/codemirror/5.65.21/src/addon/runmode/codemirror-standalone.js
MD5: f1f47322e6af5937de4a14fb10863e3e
SHA1: 843d01e1379550e5fed3e64aba1af1a359441e7a
SHA256:a18754c4ae17e27b7bba46b338c404d28804e237f41425aed96904c0aa1f49f2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: codemirror.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/lib/codemirror.js
MD5: bb40be7e0d25344024f54a03add3083c
SHA1: 0bd121218432463b298123605a1a832d40f174a6
SHA256:e98aac5ffa07bae58acd4ff07c4293059f8921c0ae0eba506929d8c6f41c9288
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: codemirror.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/codemirror.js
MD5: 0d4d22de0bcdf7f7afd8131d4e59f130
SHA1: 819f8c37a4df0c61ef735d5b884c6c598bc0983e
SHA256:b2a1b676605c6428b6dd7ce21a8a0d2509d4652ceb2297be93078ca6d66926dd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: codemirror.node.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/addon/runmode/codemirror.node.js
MD5: a524724c274d1c038c7984e164428b3d
SHA1: 18fd7183236cbf1437175c8d31509ffa6cd4ba64
SHA256:fdc02024dc3845f85b38046ae842b0f572f91adc5f34a6979cd92ead0fe4a0a1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: coffeescript-lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/coffeescript-lint.js
MD5: e852ea5b9ebb97947ffd169523eca098
SHA1: 58ec1f05cb6893a519fe2d7ad1b9716f15219b89
SHA256:824caa68710a7f931ebd30491fec19dcd2c6fa166c21158f5ccd61321069da2d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: coffeescript.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/coffeescript/coffeescript.js
MD5: 438a52e20ca46a26383d4eb6d33a5c6f
SHA1: 8dd398cbd2955bcffcd70180f9fb560f56acf567
SHA256:67792b36933d29b482307761ee03da520a19b3b30ca60f54df9cdef4051db628
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: colorize.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/runmode/colorize.js
MD5: 626a64f8687ca9576bb017843ab2c30b
SHA1: 4899e8d499849fb02f134afb39711d3ab2c28903
SHA256:9d39f5267c05d930f079fc4f223b453e8f9fd54cae6cf52db9b5dc3a0b9dd694
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: commands.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/commands.js
MD5: 9f984e904c9556f8e270502eaf1d5a5b
SHA1: d16928b2cc389c46f7b77121beb7376a50f11c35
SHA256:5f23178d2f8f62f97af955560fb192e5aa898f81153b9c24cee8ed6ac567f658
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: comment-fold.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/comment-fold.js
MD5: 3bf750756a24d5a0ba9cf16819bf5cfe
SHA1: ad4d1534287f90692567139c0b007be29aac4a9d
SHA256:a79d02eb1b425d8a4823f2d962b7b9f49af578fc9042b928b892417c00e7d13a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: comment.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/comment/comment.js
MD5: 18fc449bec0798e43182173ba47455b9

SHA1: 29442cfbafce86a08679824a999b87ec1acdf567
SHA256:a65c038258c6541658a0e9f24c56c78255e0e20d4cf06aa9ad83342069a589be
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: commonlisp.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/commonlisp/commonlisp.js
MD5: 9449ffe942392a1ad14eaa723578b606
SHA1: c734ecc91ff4949d4cac179a55bec5cee55da153
SHA256:0efe46913f843f5c335c79e05ae758e60212dde9cd3c45d99fae8066bd13c128
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: continuecomment.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/comment/continuecomment.js
MD5: 174c186ec1902fdcb1aa708a9dea1aa4
SHA1: 7c3bb959b0c3befa4395c61ee8fbba3f7f6c6033
SHA256:eb64c50f80cb3080052971bc075bbbf421ab50287804af8ce47b0536da5365e9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: continuelist.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/edit/continuelist.js
MD5: 630509c4379923d8c811b3f1acc931fc
SHA1: 09118fd53589fe18289006df5cc57b4818321197
SHA256:6ba9cd9528b74e7f76f4b9ce9ed0677bfed7057d1aade0050185368cfd0ea2e3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: crystal.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/crystal/crystal.js
MD5: 1a67ecb6914505127b7fdb5b6da0a37e
SHA1: 9123cde242e364d133d23c034ec30c1db823d241
SHA256:43be82cecd28ee92a0b7def0bba2b58408a6f7b9db96ad1e941d10d60e58ec54
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: css-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/css-hint.js
MD5: 55823389add79e8c52ffa7df6ba94515
SHA1: 59e0f4c17ecd9595fe88a84bc47fbb994803fab6
SHA256:0e22d6efa1ea084e8316ec6d5e4c809534f0e36f363bbc4156609201d95c6601
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: css-lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/css-lint.js
MD5: e392cd5f86989535e38b3cbfb5134985
SHA1: 0986b3dc26b02d98a91b91bb38d46065b5c0214d
SHA256:f3fc7474cbefded7f1b06d63efe980d58970785831cb35f29874ec371cb4ece8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: css.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/css/css.js
MD5: 3675078ada8a185a353a6560bda2d5ac
SHA1: 1045cdc88a58fb002511eb21db184ed242730f05
SHA256:60f0689e5c6af7f36c341e8e1341a4f10b4f0a04cebfb7341bcbedba9b572b32
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: cypher.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/cypher/cypher.js
MD5: 0439f14eea37e69f9bd0af1b9c57e014
SHA1: c65b82f89865edb564d52f00afddafc3d18a8d6b
SHA256:6d8c9c8993fdeb724f1f68e9574fdab0001da1d31196e33ac6112303005d3f63
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: d.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/d/d.js
MD5: 0632861907c7e77ea48e0952d2081136

SHA1: f000ac2fe16c377837034c69cdace651a45f4e7a
SHA256:8e3994ce4f507e692b65aa73ffbfd58112c4a22771b84b8ad86152578d4e8130
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: dart.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/dart/dart.js
MD5: 3cdfd4d41d52f7e80caf5dcdeffd466d
SHA1: e8b423670d328016360cc4b42543950b9f553d4f
SHA256:167d0b1d99b6a3498f6afbe6a1dbe561429099974c4a7dc682cc94832efee952
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: deleteNearSelection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/deleteNearSelection.js
MD5: 813d638d2d4693bd14f7b6490445a417
SHA1: eec62305710c8c0a032933bbee41c3fd45142669
SHA256:dac971ad5b761896b830e95f5e2240e2748fb83c909ef4c5ea4fd1f60ae031fd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: dialog.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/dialog/dialog.js
MD5: 1b33c63e7d89d740d4738ce9766b19b0
SHA1: 14cccbebffcb2f33d928c4a41d854237cda5dd97
SHA256:fd8c925fcc25357617faff21220c026bb91a617b995268d96c5d39232fd42833
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: diff.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/diff/diff.js
MD5: f80746d74770ee6dcf444e99f75d5537
SHA1: 45f65817bf0cfe00f52a620c44e48031e926e5bc
SHA256:3fd0e844e22f475503415744b7e7af24df4cd0670709c77e5e43e92185ba32fd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: django.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/django/django.js
MD5: 3c02fcac64b6100a0f369edc8d145f97
SHA1: 9ab00e90ea9a3788178187e9451bdaf61bd311fe
SHA256:71a3fa0ac63fe080a12097209e509c36abe0fde9c9709610be1656163d25a8bc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: dockerfile.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/dockerfile/dockerfile.js
MD5: 35fd7d7d73ad6c400c0afed686a383da
SHA1: b6574f6951c483c563456c9094178769ea733631
SHA256:fca390cea85e1b711389d1a91b99faeccf7b4df0f48e3ceaecf2e517982cb2b7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: document_data.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/document_data.js
MD5: 86420f7d4afaa1aa00313618bff8292f
SHA1: c26428a7245c7ccbc2da6e15ea8071a308efe21e
SHA256:bded28025266e28229d4328e2a4ff6c829e26757b12861ec0c561c495d4b87e5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: dom.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/dom.js
MD5: b78de499c0cc1d48cf541853c74c5b7d
SHA1: 1e5c213eb910d973a34f4ee7b30057efa5655575
SHA256:696b528c7a32b37c30384925dd7691a13f1f463278284df817238ab6d358a4c5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: drop_events.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/drop_events.js
MD5: 940690e5c792ff535ef797090cb7ed5d

SHA1: 05108fb9bb15e761e86ef290e006cb7c620de955
SHA256:60fa1577514a516587de192c7c779b4447aff1b6d26de0498030340e12945390
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: dtd.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/dtd/dtd.js
MD5: eb3e9b71c4e33120225df386c29a0b30
SHA1: c91a19fca8b5bb610ff35e8ea7c9190c9ef996f0
SHA256:3f04995b147addeee1637bbfd0054676e78d13f7accaf2f589c55837d70148c1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: dylan.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/dylan/dylan.js
MD5: 99e3fa83adb7b3af2e363942a5b720ac
SHA1: 795b6199d3643d0a9eb0b018a02357da66be8f3d
SHA256:999b862ebc559366e71a731e2a28b2762ae4fe7c7882ba5f6bf20c33a2d737b7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ebnf.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/ebnf/ebnf.js
MD5: 8d8a62f6874e4e8378d16d02b09ada60
SHA1: 84295b3d4f48cd3080508f3c5c12ecca2842dca4
SHA256:1175e07f831fd02ccf09d4582351c5932a48fa03be5c0eb1028c8f96c051935f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ecl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/ecl/ecl.js
MD5: 04722d23df4c17765bb397d871875452
SHA1: 63a19016bf2e53ba5c73fde154b9bbc19d96130d
SHA256:c78998872dd14cdb356d5a9bd196f7d3525e3cb03a591133e0e904afaaec11b7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: eiffel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/eiffel/eiffel.js
MD5: d202831cfe3aa85bdedffd44534dc98e
SHA1: e5767dbfb329d8e3786acf893d038e1e4dd35c39
SHA256:183e855f6474cc2c4cf0b6c5e5c40ea7821707d37ac414277dcda294ffae1721
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: elm.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/elm/elm.js
MD5: c37089c171d4384ec97f9af66d5ac972
SHA1: e28a667656ac12ff06766d2ee857962dcd9146e2
SHA256:e343ffaffff2dc6fd9c5923228b46c23723c396993459eca6217871f1c087ebc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: emacs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/keymap/emacs.js
MD5: 258e09f1d4cdb812940d869afce12a11
SHA1: fa3b963c38f809ab13c37fd7aa654ac46a39e740
SHA256:af2f42c9f461951f13e9785f634cc9f8e5d63b0c5c2375b331105dea19a71fef
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: erlang.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/erlang/erlang.js
MD5: 29f92a4be923242d30cf1f4288c89adc
SHA1: 45f94b33af2bc74d8c5eeed73de27eb8a4047c20
SHA256:2ae29808247e9d6a58a83893b0e8b627c0ca337cffa541ef16fb506edfdba77e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: event.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/event.js
MD5: b700f1676589e7f88e59c943cc209156

SHA1: 516c718a9b2f86f68127680267b92d10fbf5a579
SHA256:1b13113fab8763c3c9e2284d1b6bdf1f84ab3424999a2eacffbf771ea8b75513
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: factor.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/factor/factor.js
MD5: d497dd1c4f0f85b83245bfb80943e5cc
SHA1: ec2430a02377f3b14692370e329b8f83b017d1b9
SHA256:baf7c16c387e7abfc308dfcb7fcc1ea9ae0a898d13455349083ea72c7bfa4c4a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: fcl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/fcl/fcl.js
MD5: bfa4a30d52fa501346b203c8ab6aa0cc
SHA1: 9befb1efc7f051c189e1c2c7cccd976576bcefca
SHA256:7c9d372be44c1c418a101885662d80d4bf6104e1b717d36cbdbd05a5956abc70
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: feature_detection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/feature_detection.js
MD5: 3b63813f217d9351f7a1d90edf345310
SHA1: f236ad77f54768dfaf4b78905be71b6873691698
SHA256:4aeaf197f379b3450c8c297f23e449df3795a9954bec48cfcddf4b3615d5f371
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: focus.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/focus.js
MD5: 307daeb9d6322c3905fc5b2ba846fa16
SHA1: d1e1cceb41ec90a9b18fd25ae6cad9805e86811d
SHA256:2f6ad1d093d5d933ad58ded481d34002320d2887b5d06badb35918289338757e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: foldcode.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/foldcode.js
MD5: f520bc635201c451609403065b8bacfa
SHA1: 78958ff57ef86b84ac8a8085a4f0923433eea9d3
SHA256:07f353e02abcc300739b09f31a9d32a958ebe5d2f76959291e5643c6e40a26a5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: foldgutter.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/foldgutter.js
MD5: 99fa4292c7007f77f7061c6b3a30d3e8
SHA1: 33db6195e0d5ef96a74fe770cfae60bac35e6cc8
SHA256:5f8b148eb046f946dac3a22b4534fd30ebca826223dfe291a49345b9e2cb400f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: forth.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/forth/forth.js
MD5: 3e09048506ea36823a8a5e6ad244c7d5
SHA1: ef3e2632de5a4c57f8b14225026940309167d270
SHA256:1c6c0a8fb3572fba544083795b3259f8a35cae81ec2ddb19b4fd7af2a91ab34a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: fortran.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/fortran/fortran.js
MD5: acf9c5ff78882f6ee77416eb957e881e
SHA1: 30130e625c08eedd8d62021c0dc77a71d066fd1d
SHA256:b3351c6cd6e696c2ebf0e6ae1ff7925ed65add92947007402e0b3112634f6392
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: fromTextArea.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/fromTextArea.js
MD5: 7df499908f8c35dab896ef04aaa99608

SHA1: 19c78456369c4e1066ff8c509a8fab8ee5be4ac0
SHA256:046189bf0bda8833502f6808c0429f58383ce3c3dfec42a75de4a0b1b1879eaa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: fullscreen.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/display/fullscreen.js
MD5: dffe3df188ef201ff7f04977d0ead894
SHA1: 29d2bbd2368fb2dfc02a06aac6db6aa9691ab330
SHA256:8e4a21aa77765df8893fc854c4b6be56279e12d9a70cbede913083c307ac769e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: gas.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/gas/gas.js
MD5: 81bf6c3fbf62d42e9c07b99a78164196
SHA1: c383c28efe0564f2be8433311d959f905be82a15
SHA256:7e8cb40e5de17ff26a46cd1741a1923cd6935c3cea9aa68d3a2683f9ee4b3882
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: gfm.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/gfm/gfm.js
MD5: da48b005ec4e651d019aa09b3d6d4aac
SHA1: ea5f855ce519bf55f09cb2c968dce9660615c698
SHA256:1fcdbf9a611c238acf53f906126fba93ae0550d74858efad61d72b8b3ed6e0bc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: gherkin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/gherkin/gherkin.js
MD5: 2a3fb5426a7e6bcaac13011a8f702d03
SHA1: d4b7b4d5996deabd5a6dedbb86e52625cb4f6a4e
SHA256:13073d40252135822e958fb11caac101d98f20c0ef03a572084e03f2df2f5d9b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: global_events.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/global_events.js
MD5: 288615615004321c6abe2bf66842b8bc
SHA1: 858b4b90c061cf34960b0bd4231a2b7dd7ec5f3b
SHA256:fa803fc7e109d232afd12dfdf4d99adea71081cc4b71e547d4b1c2bf46cc9ca2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: go.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/go/go.js
MD5: 13b22bde61623799e7801dc496160da6
SHA1: 33b9c7dfc7e5000a5deaef2882702fa306b58d61
SHA256:a3402cad4f69a45992d8f22019f156c560c1d8f06c82d7cbbf4339f2745a6b0d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: groovy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/groovy/groovy.js
MD5: 10976ee5ee240453070e5d6166a8902d
SHA1: b77c90207414765a5af7bcf7d9c1dcc75ea5f600
SHA256:608451c346a072aa7b0f6851e0bd45fcf9ccf703a8d5e641ecf9ffa653986bb3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: gutters.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/gutters.js
MD5: af3de2621d2ef402646889be16bcde7b
SHA1: 130d94f44dea7f614a15009677e496ad2b853025
SHA256:2143db3d42d9a3408b556eb50068870d138041a9b98ab256d070d982e09346df
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: haml.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/haml/haml.js
MD5: 7d65bfd39de90f56597eb8e278a39af7

SHA1: 7bafda0fd81e500fb2f364d2e657fd9dec939505
SHA256:9e9606fecf19869e51c32a84e18c4447c0d4ad2031730e5690b571f318409022
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: handlebars.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/handlebars/handlebars.js
MD5: efacd8d006bf9f83baec2fc5a8c71feb
SHA1: 7fefb944ec70e00d262252956fdc71f04c1046b2
SHA256:60bac3d6993264e155b5a06f52cda56b7bab2fb5923f3d1cc7e8caf704fca724
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: hardwrap.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/wrap/hardwrap.js
MD5: 049ed63630662fcb8a977fa43f86e058
SHA1: 535a020f7839e52da6fc7b8af3d249f641c5e055
SHA256:bee81aee6222a46b1aeb14d6fc738d3cc09a4e421f808e29b3c6989710ccbfc8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: haskell-literate.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/haskell-literate/haskell-literate.js
MD5: f0bd7313413cdc35018db90a6522d1ef
SHA1: 670b7735a8c85e5251aeadf51f5005d5cf45df44
SHA256:7519d0b515603244f029c3031a4625fdccac88cb640fcb6e117718ec2c0b3c50
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: haskell.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/haskell/haskell.js
MD5: e4f82d95d10c028eebae3338e678be22
SHA1: 30c46651b2b0b5a7fc70910b22e52e2d1d8687ff
SHA256:4745a90832e950c9536f0bf498e5bf6fb3753a4a98bea09ec152b92354c0fdaa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: haxe.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/haxe/haxe.js
MD5: 13c21da31a992b536d4f37ee53e09605
SHA1: 6a694b4a0a68b148e0b2e0b761a521a5fa4a0296
SHA256:f3596c7efe948a3331bb1bea299f6fcb8e7733777dc2114a9f2147dfc1c69257
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: highlight.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/line/highlight.js
MD5: d7710bcd63c26c5fdc37c19b15e02d4e
SHA1: cc5bac275e64696339642c6f5a52c254f139fbfd
SHA256:ccf8b3a879acfa0013ee5b11e036b822b68ec5a136c218400775fe2e35a3fd9b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: highlight_worker.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/highlight_worker.js
MD5: fc6f314859dad397c1f867ed5d73205f
SHA1: 80e56feeeffb3ad7b76e40dc4577962a60becc11
SHA256:fc9d8bf90534b9a6c7d5a45e8f8f79a4f8827a661c4271f812776e7c3d2bdc09
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: history.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/history.js
MD5: 34cb233d1bf8cc676a0c5fc9e9c24b04
SHA1: 4c42d70f020d1fd9397fa16ea34f5cf54487e93d
SHA256:961d52432f8f463614f83e660c2945f9bfbbc9c8fb7767575b9221c3e88821a2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: html-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/html-hint.js
MD5: 609fea85a7894f8098719813c58219c5

SHA1: f593de64cb802e0e456482b88959a68260e06bff
SHA256:64d3ef9293ed8917e40ed4e8196da6919379a3b4970c007785c7ed27ab9a0478
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: html-lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/html-lint.js
MD5: 0844a30ecec022fb60101fc0cc6a5cfe
SHA1: 3ed8b2f11d4c7462cf29fc93b58e579680bcc32f
SHA256:ab7827913934f06a8b4d00e41d5954974c90d5085d1295fe02c484c782c75843
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: htmlembedded.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/htmlembedded/htmlembedded.js
MD5: e7a464409318dee8c3c6e0b68225d461
SHA1: 548ebed43650c26970abca5933aa237b4a1950c5
SHA256:8afc8da4e446322cf92d78bef9940f9444aee339f56c8b9af5452fadfb867601
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: htmlmixed.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/htmlmixed/htmlmixed.js
MD5: 4c5a6f44d738b718d1f6164c1c8d6904
SHA1: a4f9c3552740fb908e14fb0f47832d10a3f535d6
SHA256:fe5912e1d10f8fecb98bd31e2f957c0bbc9abf6b505d11b6dbcd27542d0fdcad
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: http.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/http/http.js
MD5: 42dcfb1c4b83e85eea0303f75a3f08e1
SHA1: 7fa224e2e3ab674ca61cedd48fd430c5e62e1218
SHA256:89842864a707564a989a841ce934b61659f34b012f2349e5c4fd9a09c5982f6c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: idl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/idl/idl.js
MD5: 1ae58242a3b61aae5bdc5665bd5fc2ed
SHA1: c25b0c5644c33ee3993ee3152df8f4c27235e172
SHA256:7d45bc0899e019f558e68eca684ed84660bf4687cd64fb4ed2c959ad249b763d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: indent-fold.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/indent-fold.js
MD5: 623d14360009d84560611f43b83e6759
SHA1: 731e1d84971dcafb20d1417761c18c55883c3d98
SHA256:a835ed1af176b96a1bf00379622e76573a1f6327bd76b583d9c4757a2c4a4194
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: indent.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/indent.js
MD5: 835649b199c40a992e89a61de3514147
SHA1: e3d98527805fcef17ac4f710d7600fe0da52db33
SHA256:f28260cac8eba83de19891709eb8545ecaa6cfa3ec716e617992e14cd0112404
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: input.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/input.js
MD5: e5b3458aebec88bd62d53ba9503f3dcf
SHA1: c12b0be3e1611d8b1d357d8169f3c2bec3b2ead0
SHA256:264da6a7dd800f16c720200cd24f4017027fcfb95773ac08bdf9951b22fd0bd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: javascript-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/javascript-hint.js
MD5: de72c8e29800ee9ae93e5c8a43c6c6a4

SHA1: e348c54c78f75047c06629a13422c0aee0ee3253
SHA256:e4dfa3414b3b9535514737074cec2fb0cbf0bfea7e765307122295c98c5137fb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: javascript-lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/javascript-lint.js
MD5: 55eb8a1558ef8c9da7d355a32334d62e
SHA1: d452acc1222c992a222c6c4bc55c0546eb2a465f
SHA256:69906dbb83d60e0d104ddf395e29dcaf4a05063f24c085975b9c09693dc860c1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: javascript.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/javascript/javascript.js
MD5: 983beea4e8a4942a9d3e92dc097768fe
SHA1: 5dc646acbc67a46801d15f6e5c80b9ad620ffc18
SHA256:1311c73c66308ba6f78512b4c2e770a6900c80c3629683763329668ee6111163
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: jinja2.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/jinja2/jinja2.js
MD5: e7c1e34ded0b99a7433a47f170932f72
SHA1: 0e5dfa653ec704c7aaf3c9acd58fb7e0324e77e9
SHA256:037860e24dfa4c5a27ccc3d4a0383ac500332955aa336947f4133cffa57e4e13
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: json-lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/json-lint.js
MD5: b01056a065c6df2ed0f61038c88e5ecc
SHA1: 8fcdcb87fd1c9f8fc04f3fc325fa590b27441183
SHA256:cb3522e1bdffb075461c848ba2091cc781b52ef0e69cb39d9a33e1b74dc35ae2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: jsx.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/jsx/jsx.js
MD5: 5b03b29711fffe9a3e63bdb637a5686a
SHA1: dc3a176ac8de36e56728218ef5638042825cbe0f
SHA256:2f008854e5d215d38032d88b90594c61970de3725802f0ef6faa0e70316e9b74
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: julia.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/julia/julia.js
MD5: 544d9103cd9877e0a7dbb26dd5a34eea
SHA1: 4d6fef3f38c3c9717b6ac72fa4fa3c6d48ca189f
SHA256:54d93c9a83269af3bd8bc6593be2368f07b4efa4223074b54f3aad44097a4d32
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: jump-to-line.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/search/jump-to-line.js
MD5: ae33156dd047f75a6d2539b21ac92df9
SHA1: 4b8098d4df0e0bdbda6b27961ffc7bdaac14e85a
SHA256:39b7d80ee80cabe2f5936673b3cadbfd4d260dfe6dc6f936523a334044962ffa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: key_events.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/key_events.js
MD5: 2175f6ba67795e9212824eade6a5da9d
SHA1: 5cf8f5c23141ab9cf92c8335196575823b16cd4b
SHA256:4eea4b33d8ce96aa1133e73ddd752756da93a1ab8ebd11a71fd0f6abd5c39d72
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: keymap.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/keymap.js
MD5: 1c8d554d0dfbb08ac3b4ff11303f313a

SHA1: bcbddfc0d1411afa8455d75564758dacde1e15d5
SHA256:9be4f88cba00a971a1a007ca4fcc56f244ac84fb8b24f165f6ce2793c2f83a95
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: keynames.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/keynames.js
MD5: e4ae7351260c5e7b9f2253e21b5ca9dd
SHA1: 9b6381177e6d4afdd03388c548a00bef7e101b0b
SHA256:7054358c3e0ad3945e0c3c31fde7b77d1af78874a5fd436a908aa0e8eeab7b03
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: legacy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/legacy.js
MD5: dfa5acb74b48161d442a6d83e1abbc03
SHA1: 70f5248919c6a806ec8da7a53b9167ea0d28f28e
SHA256:663e30df9fb1f4994092c95d5a4a2a127d67d59896b4795807ac912773a759a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: line_data.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/line/line_data.js
MD5: 0239405c8ea2b45a5a3a2de75bc481b7
SHA1: 936ff2393f4614f8fb907274c896d2435d34250d
SHA256:11203cf446205f30a8eb2f5633369c7a6c00cc778b3cdbf1da16570571937d92
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: line_numbers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/line_numbers.js
MD5: 22976744e5315917483bef53cab4d368
SHA1: 32c75bf2e39c2315fd1a1d04cbcbddb666c998e0
SHA256:2474c6d14659ccbd6664aa88eaac7f1bb5589cc44f5acff4c5d8a22ed5da5d4c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: line_widget.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/line_widget.js
MD5: 2a58b1a6d7eadb596d3968096f1493e4
SHA1: e06ec6ee060c9b180dd6269107c1643618024acf
SHA256:4557109a8ced89105c13e911cd0d4036a043ce83abcfaefe9b6889ea8d058b16
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/lint.js
MD5: 1a03065838fe9b18a91db3bb2bf0115e
SHA1: 0a89fcd3116aace99d94495d520552a6b01783e1
SHA256:8d16a6b48b5b860807aaf7c329009d7a49f8078570263a6def773c61d2b353fb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: livescript.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/livescript/livescript.js
MD5: 303cf9371fc666702d07b7892d4d69b8
SHA1: cc1a29423cc292dab8ceccbe8d1d4995426ce11d
SHA256:b9b5f3fca094c735f94174d463746bc39d0930dc42b70bf5004efaed96b080ea
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: loadmode.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/mode/loadmode.js
MD5: 43a51215f06278be12990128bf16cffa
SHA1: 62a2787a4f3b623af185185edaedc7eaed7ffc08
SHA256:be81c0312e7041f56c217430a177fea61e572bcb9579a39ca1922a2e4d51abec
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: lua.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/lua/lua.js
MD5: ccf279dcbc882c0e99fc9dfda9dd734d

SHA1: 13ec1f41c7c723c70f185f6c22e116cdf532d8dd
SHA256:5c702747f50d5d4158ab8c096b33a7e0092529d5682a728a20624b01dfd86e2a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: main.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/main.js
MD5: 334b819c6eaea05be03b18ec00f12dd1
SHA1: 860dff15f1788b87af4aa9e312c3bd5da600212f
SHA256:e24dafe26af2e9eb5c85d7314a768c4fa16ebcfc40172a7220ef91f1e5b18710
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mark-selection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/selection/mark-selection.js
MD5: f2b8639c24afc6cc370f4097eb6bb217
SHA1: 62883a7928526106b19fa78a1195fadf463550b4
SHA256:5b9c6a0031fe895641f2eb2198df2592ec769a6685d6bb10f3f9b92a7822e286
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mark_text.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/mark_text.js
MD5: 7611054f886606aed04a7a3f3c4d5a78
SHA1: 3e6ac9ae6a89f720e9c148d25746ff37f9207d07
SHA256:b17ada4f3979fa8170a4abc071035badcddd87870a212cd92dc5b0a70fac19e0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: markdown-fold.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/markdown-fold.js
MD5: e9844099dad7cf95607a804988677f22
SHA1: 400fdaaf493a4d15e10b397553549b6b4e09dc92
SHA256:6a81721447c7260578e8e306c89b33a49e98edc1c2cb0c52a18ca0e913684d96
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: markdown.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/markdown/markdown.js
MD5: a7326be775e85028373f9236c26a572e
SHA1: c7dda08f12cf129cba6b317f70ee7ce0abf775b9
SHA256:8fe7b11848f79cc9119b2a239f38a00944f6f2bb764a00bc837ecf8d34cf7690
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: match-highlighter.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/search/match-highlighter.js
MD5: d7d3dd2592e2df81c743b86a46ccc555
SHA1: 21bd58338eb506c53cd367b4e30c6aefa2e7edee
SHA256:8c3e196f9a5f9e5cf9d7e71751132a05293e7cdb180defacf28be9fe919682cb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: matchbrackets.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/edit/matchbrackets.js
MD5: 82000f1a0a6dcf462ae45f1cb9aebed8
SHA1: 101ef35596117c0ad4275a68526eb7b65d810258
SHA256:9d23a177f1e4d07e3acc37c210ffbe4c1c2eb4d55bbe54c16d3e7ad3d04d0401
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: matchesonscrollbar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/search/matchesonscrollbar.js
MD5: e005f8b0c7cedc509a29ea1a517cc829
SHA1: 73a8bbcf26072f44bc7003faea790d1f3d59096f
SHA256:a2deca7f8ca380dc7772929cc7c23b6737109f3cf0a55e7e18832808d98530c8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: matchtags.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/edit/matchtags.js
MD5: 6e8c7c68653d8d6b912138fe6f155e1f

SHA1: 99f7135d209eb1da2c326486eb53ecdd330f0f2c
SHA256:263d752f850b20890f0506fcb277b094b474138692a58b45d7b9bb03e20aa00c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mathematica.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/mathematica/mathematica.js
MD5: a8c37dcebeb98162e29e9d1483edf7c4
SHA1: 82d9653bf7ca5b228759c5ad53845a8237625792
SHA256:a301011fbb5d9ea4f39fc574718c2d27afd9425e31a1a5bf9005617603b45c0a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mbox.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/mbox/mbox.js
MD5: 9ce449eaef8f2c3e6253bb202a3da0d0
SHA1: 6848c5a33d4ea2c76fc6abb4fdc3c9253eedbc9b
SHA256:9affa80931d9bb09746d08b9b0f90286d2b47f5b16a0bd8a1a06227b496c4b07
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: merge.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/merge/merge.js
MD5: 59079d3cfda5a55fe7dee288eb82e4e2
SHA1: adba0ab1da8dea1977e1c209d2fc05bd3f082eb7
SHA256:e6bee9d4720f751038126809938c66199c7a5a4679b695b0db60302ef9dfbff2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: meta.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/meta.js
MD5: 11f14aa114ed56768aa48301be3b9f03
SHA1: 516781b99334a9aeaed0d9f1b9463d8330d00ab2
SHA256:f95786f9c83e631225fe7866f39892f808aeb015e80ce9d8a58d5a1d4e9c4bb6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: methods.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/methods.js
MD5: e3a7acfd519348508c4b037bb91de3c0
SHA1: d542679673c8db6735ac1e43172c534ad4c1d6a0
SHA256:d1919070e189cd98126f38a29b1e352661c5ee1108f93bff8ee282c6fe3ed6ac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mirc.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/mirc/mirc.js
MD5: 23555fdd21b7305d57c24d1378a03754
SHA1: 373c327846304793f8016feaa0164226d6fd5020
SHA256:ac173799c5f81a8c8813a5b0c20b700b27a1f571d1e70132e67d8451c3efaa5e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: misc.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/misc.js
MD5: 2ebb8004b5b9b9aebda4fe4eeed2e758
SHA1: 6f99a6326333db85407ef153f941bc06b9f3689d
SHA256:5e5b704d870e34607456680ca283ace3b4e93c7f99052bf5af43b18bba9d6c40
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mllike.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/mllike/mllike.js
MD5: b30e7da7837eee7a5966685fa03522f0
SHA1: 648a539e28df2714182163665b797d783cd47d80
SHA256:a887947e50c37db0215fa4076c3b211093dd9abf643518a2f304677bef848211
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mode_state.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/mode_state.js
MD5: ffc05060eaa3b3d89beeaaae86b0483a

SHA1: ad4db1fa999cdec7dca274bc0d440b9817706fcb
SHA256:7d986b2f9cea39f7829ffd57fe70a6d891afb68bda46557f3d361fce6abddedb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: modelica.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/modelica/modelica.js
MD5: 9d173268d73ae885e07741f6a60913ef
SHA1: 2cebfe05d43ff1b9a4608bde365d0e340b9e2b08
SHA256:96befada89421de8d32f6355c326510128e429167390c60ba81d93dfce4b360a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: modes.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/modes.js
MD5: bcf367e11e7fac26e7f1668e8f1d1968
SHA1: 26c51a0d675e8420deabe41af39537b98b494f6a
SHA256:faf6b57425b7b95a14650da5da6a488cde013e23c1ca57e4223146ccd369230b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mouse_events.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/mouse_events.js
MD5: 59d18eee2c7dd5bcec2d1ba234cc5597
SHA1: 7a59397d8f1211d492b023ae472a44a205a60f32
SHA256:a368e128f10bba56db3d5325586be687f42c4cdec1de81aa4167430174de8bfa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: movement.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/input/movement.js
MD5: 386a27ecd12315f9eff836ce5ab2091f
SHA1: 3170cd5a925774250a79d9e1c9130040e89a6be8
SHA256:45f4ab6d34f817b4d945449664a35848a252a87f7aa7e917cbefd5710cc06334
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mscgen.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/mscgen/mscgen.js
MD5: 8e06dd81adc9a26c6c708d253868c290
SHA1: d44dd69d6fe4e456417da210928371090d426921
SHA256:91eff4cccc80f0048d1f7efce0197be483a013dd299e2718b49315639a3d4885
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: multiplex.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/mode/multiplex.js
MD5: 0bdb637f0ca08689fe55e572cc10ab16
SHA1: c1eb99a3fdd03722c84c78cb9351791428ff0bbe
SHA256:09ec21386de4e951c1eefe0f1db478a9f57701b202ce18424f2b89d4f74aeff5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: multiplex_test.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/mode/multiplex_test.js
MD5: 8a377bbbcf33896551524b1ccebc823f
SHA1: bf15c3dc16b8de593577266b9ef1f5625d67a0ea
SHA256:73e22c6765036bce1db37e31f8c46d62a56ca232840fb4fb968d17c24c3e8f74
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: mumps.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/mumps/mumps.js
MD5: 8e0c6375b6bbe74f633feed856f4283c
SHA1: 6944b10c9a28d7097d90291dcae08e9924461140
SHA256:1455108cba483e767bc5072ebda6c4c219395adb574aa70f7d7ec856225c3d42
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: nginx.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/nginx/nginx.js
MD5: 63e717882de52ba3a4bb62c9e7bef83d

SHA1: f008d01cd0b803de9bd5bf1088feec56c6eac9c5
SHA256:e35111d1834678cd34bfec04abe169cb11739f39750d1c41ab57c8f2524748fe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: nsis.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/nsis/nsis.js
MD5: ccb0e38b9b3e49ac793f44b8e5d78037
SHA1: 38673a38900fda3fb7784b9d7efa29482e4383b5
SHA256:d7bdb926dc600828bd1a4299a120561f830773f3c6c272e8c1ef8c814d1bed1a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ntriples.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/ntriples/ntriples.js
MD5: a21f011183564e5725ea16a6ca11b089
SHA1: 62d7d39e91ecca5bad75c91241aa31421a303ba4
SHA256:d7a1fd7fba26679ecb0a6ac0b67164ed12a37db25d32ece3472920c6f25a74cd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: octave.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/octave/octave.js
MD5: d830f31f1647efb252a53d0cb1f18aa1
SHA1: 1abba38966f306c238e8f9cf168f95db0e16d5a5
SHA256:b6c6966b9a564ceafa2b2c5ddde2f2efb0349cacdab3f61d90fce2544ece8615
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: operation_group.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/util/operation_group.js
MD5: 72f0c675f45f87c9a45b5f5784212fa9
SHA1: 8ca609f3cf238954efccc55c720e733a56f5029d
SHA256:aaa9c34bd1240b164897a412a257d2e693d2ad35bec219cf8959561de6559edb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: operations.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/operations.js
MD5: 497461c43e61c092dbd129e3e3c49979
SHA1: aff62b3e7285e0e8ea7e97960b9f74db22d3136c
SHA256:86cab4723143b0f59a5cfe2bc6d7f89374bad65d27557349ed16ae23f27050be
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: options.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/options.js
MD5: 7dc696b83ba67a775b55bc5c07ec4985
SHA1: d732c1c65a7f2e9572c486fb2db1baace52ebbea
SHA256:364c0df16f422ee05033b717a51f5d9fc50afa6895266da13c02e311bfe087ca
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: overlay.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/mode/overlay.js
MD5: 3cb76447dd1f64cc2bb037f3ec8c88a9
SHA1: 1ad72da6c675d9b6074f69404c66118ff24389c7
SHA256:1b44334e2a04d90f2b473c2684779885903919014 2e53f72f3b7de0f82696d0e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: oz.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/oz/oz.js
MD5: a097901a9fe996b190b9103a64ace0c6
SHA1: d49b86c59bab331924fc03e3f680af92a6bd79d5
SHA256:641554f9736e5260ff1aea064749a590cba2a854bad6fc334db8ffa2bc1a6892
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/package.json
MD5: 279c97c61f449ff8373b97074dd670ed

SHA1: 468d7998fc7dcea4886c3a9db48ebfff9cfe8811
SHA256:95a808668722f226219643949ae753d88d730b370c8b3b6f5decdc802fb056c0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: panel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/display/panel.js
MD5: f647c5e58b5c032c1691693333104941
SHA1: 5c8285f946d9888b499ae0266e8e165696947074
SHA256:2b137f8e8631c717d2af81edc341d436cd3a6debb8e9fdfdc20630296685d3cb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: pascal.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/pascal/pascal.js
MD5: 840bf470a5371641f1d5834fe891b8cb
SHA1: 8abf78c23f1784dcce527dc0021c1a3434b84d6a
SHA256:b5c7e3014cef30b9929b71dc00a0ee7d7f323bc1f6917d02e21dda45e0d5b928
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: pegjs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/pegjs/pegjs.js
MD5: d9cea74c276abf75a38bd132351d9257
SHA1: 5911a8d96b4e99905201a22454270c01ade941d0
SHA256:1b8295a2919e341afdc7fad202335b00b93f7a01143cd509f0f932d16f567278
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: perl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/perl/perl.js
MD5: c6a3b40a8b2971690ff06860516bd140
SHA1: 08bb3e219af9990114dda08e2ad935c5992dd39f
SHA256:a614830dc6e71770cb4feabc487dfa1b72e29444789b94d1bcad62490827ca1e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: php.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/php/php.js
MD5: f2f1668dbc8a4b0fd9f031dceda0e4ab
SHA1: 31d6961d6d4cbe7bf5deb2f0b5ba099c49e5c962
SHA256:07819ae34d5830a3cf040e1904d4b641cb70142845394211f7fb63c891d80945
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: pig.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/pig/pig.js
MD5: 40f967482626259f7cdfb972548743cd
SHA1: bd2d7d6522d69e9849f8a6cf3b631ddaf50a091e
SHA256:e9a9ec475aeee8b2f75fd1c8a58ea0a2d0cffd383b1a3fb8bdc460881d612352
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: placeholder.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/display/placeholder.js
MD5: b5b4d8391f1b94044cda61cc979cc772
SHA1: af7eaa5519c4e0fa823224593b0ae0b7fda73a23
SHA256:44619626e2301fc16ebade252564e2c064113483e02f2fc8d8d262aed2485b9c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: pos.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/line/pos.js
MD5: d1fc4bdcc5a93ac92f4c3c9cb34bd220
SHA1: 810afb684197135ac8ac6626a4a7eebef9ad5cc3
SHA256:b708bfbb9ce809d5ce2d1490d806933fad9b471ac63e0f4c72a31ada57e05f9b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: position_measurement.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/measurement/position_measurement.js
MD5: 6c17908c000f5a7beb67e75b1340c3ef

SHA1: c5dd40151e773a61694906cf92f941fe27ce51de
SHA256:c5c488b91320e33d6e25fbb8ce4fbd3c28621511328b48e9690f797b81d51c32
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: powershell.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/powershell/powershell.js
MD5: cf3b0559e54ae537a420d86a07b441a5
SHA1: 992cbac5ee6c618eab5f646438ba5fb54f66cfe1
SHA256:9530fdf52d164be6d021a87de567acb8738f86f6fd98577533a9db3545e873c8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: properties.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/properties/properties.js
MD5: fdca15c3c811413459ed12fce119db54
SHA1: 715881cc0ccd13302e302dade67f675d37cfdbd4
SHA256:3f85f36e32edf82eba526ad56edadf04c33864d72bf0cfae2592a490530a4966
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: protobuf.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/protobuf/protobuf.js
MD5: 3e57a349742d01647347b7339572d9fe
SHA1: 909346135655b3aacdb909a19acb59876e2810dd
SHA256:93d1459ed6cc4e2a4701fc17959fe7f56b797d1d35b47f44b8030c0d19adf5b3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: pug.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/pug/pug.js
MD5: 63473aabe4ad7435cc804132bf743ec3
SHA1: 4e624a3174fd238241f692c1f935ae75d41269f4
SHA256:1f9e975ab889f6dd9183758bc7b454224dd11859b8e045ce5b98e2c4a05bcf9b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: puppet.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/puppet/puppet.js
MD5: be03e9aad763ae4b5ee3d6a226aa8c78
SHA1: 7dae96b96e285c5e747624c864be8f1b0cb61e5e
SHA256:237b966a50a514c6beabddfb83649797f764a29f7f2c7100dac1f411709040af
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: python.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/python/python.js
MD5: 4d1f377baf6e218d6033b8d707943103
SHA1: 18c8234dd80a098aef0a219187e521138ed78a6f
SHA256:19a59ca387addb04e95002c9adbe2b8c231427ce49369ac537107e3088a6947c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: q.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/q/q.js
MD5: ec0a69917f7ff85ef3c89ab34cbd0ee9
SHA1: c52261047f62fbf5a52a2fb36e0e926859505ac3
SHA256:1fecda8902c9c63fa36833c073370e479c7b8def1b883147c364f81cc6ac9171
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: r.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/r/r.js
MD5: 32999ceba0af47e9e6b4042314e2cdc0
SHA1: f044c32fe6998d6c6fbf774910766fca456273d5
SHA256:d4b1d1ad4275187d4f371fb61ca77ec10f63deba233644c484667750f934b23c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: rollup.config.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/rollup.config.js
MD5: 73a1da56a828ad2854d28749fc155632

SHA1: 48bed29223b72a22a9939b57333c2d6e58bdfd39
SHA256:8c887c6ebd69fc77f4d1690cc0eb5afaaad25f0e18baaa5c7fdba16a6618ee08
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: rpm.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/rpm/rpm.js
MD5: 5fbb2d4919f2d396e78074f4c98812c0
SHA1: 719d22639e2bbb16d80df811da20013f3998c42b
SHA256:5e8a8253eb986b58fb170e2d58bdd134b05fc7dc02a456374a034d7564f77fcb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: rst.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/rst/rst.js
MD5: bd89a589282ae08505026ef31cd4c6ad
SHA1: bfc1dea7ab7b49ed20e4127add87019c8dc56850
SHA256:b50d542cf38074c392f7fde44ef2cbab24b45bbfd178c426cfef6848d6d3e90d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ruby.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/ruby/ruby.js
MD5: b0b2ef072186390edb0444a0eb2e315f
SHA1: d63568f7de026f9c17e0a4124161ad5007c0c709
SHA256:953daad8a24225d56733f77c0c4451cf05436f70ad00e5dd1618486a1d5e01b9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: rulers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/display/rulers.js
MD5: 267bb54847534c8bfb41dcf227f7aeb0
SHA1: ef8505818354f0e8e79d6ef7a902ec0feaaa0ed7
SHA256:175d32d6794e2d917f446c4bcc8053c9a9e69eb9fcb3b805daaf015189b6ec03
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: runmode-standalone.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/runmode/runmode-standalone.js
MD5: 33df1dcb939ef0623470f5d4833159eb
SHA1: 7f880bcfcfb0fb23755c18c4025de22d160bedd8
SHA256:6ab4cfbcce03ceb5293725f12abfdea2a4b3999ef22a0deca5d158b87d715f79
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: runmode-standalone.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/addon/runmode/runmode-standalone.js
MD5: 8bb22c65e3d5cb3b6466654c7c6ec4c8
SHA1: 942779dcd636d8372e9d8c9949858ea5b68bfdcf
SHA256:8a06491ff4969718a7bbe2f8ae9d380e9f05f0947d7f5e0d940930e5a929e469
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: runmode.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/runmode/runmode.js
MD5: 6b9c51f3ec2f5a79c75836a0f75569c0
SHA1: 88d7a8053ef7fe9996f63800076992a5f65c4dba
SHA256:920d8eee55e987468236ba7ed2886de0bb8b2fed9d7060383a39ea29924ae885
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: runmode.node.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/runmode/runmode.node.js
MD5: b16ad3a5820869d19e1c08d921f21e0d
SHA1: 86abc3ff5a357f51f53a7a8ed458aef7a7f7d77e
SHA256:e42b873d75f330a7a30bc325795827a883a18568a3f94be4fcd18a4125645089
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: runmode.node.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/addon/runmode/runmode.node.js
MD5: fe41270e99f973a568d5a823cd6e2bfe

SHA1: c78b8d45e3db1891ad28f93b64ebd5ec6d0b9c98
SHA256:016bd87dc725d65c80cfa58d2e58033e013e703878cc05f322f938d58ddbcf9e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: rust.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/rust/rust.js
MD5: bfb43032004a8d5d115c6b817cbbe2ba
SHA1: af76d8276b553e168b5fab49108e715452cff07e
SHA256:797a9abcf8581f192bc49b11434346d3f8014763f4967ae260fbe31f25b2bdfb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sas.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/sas/sas.js
MD5: 46f6d321e806768f9ebbc0155a5f9807
SHA1: 441d94bf2da7c5299662ba76dba352aac7df705a
SHA256:b69f2877e395b89682a4066f62f686c12cb66eac441b6c1d3ee15d5004859f43
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sass.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/sass/sass.js
MD5: 0067718b0d6fa922bcf032b58966c3fa
SHA1: 1dbee553e6dfa3d57a3aa6548b43a753ccdb7380
SHA256:01ba99f4a91e70d2a5d3ef881c542f14a1f59f3ded58672484bcd56b41921866
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: saw_special_spans.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/line/saw_special_spans.js
MD5: 72b6184ab657ca37a0d984dc73e7088c
SHA1: d84fccefe8c3cd0f1a0b5b2f388de87e57503df3
SHA256:fb122060ec500dd99a179c002fbb6a8709eba030bf8f7695d868109b470b31ff
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: scheme.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/scheme/scheme.js
MD5: a64f664dcef608b26dea48b1ea52b622
SHA1: 1e90715a9ecc9c8cc9500e9b064ffe0defc60b9c
SHA256:0bc81b318e12c7c5bbd94943d9d64cf1a64674c3bcc7057788ed1ade8701ab80
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: scroll_events.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/scroll_events.js
MD5: 8c96ad450d94581a7a461c44fa1e7cfd
SHA1: c92034958533fbaa6512c99d715a6032d43355b0
SHA256:b0472dfdc7a904f6a082f064c9384dde3ce1ec95953d9c276216424da03ffa01
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: scrollbars.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/scrollbars.js
MD5: f06876b47feef8deb64e7cd59d76ab1f
SHA1: 73c1a417818efb800852fec0742136fb1c891c1f
SHA256:11cdff1fc628da528adf11b23bf19cc06072bb573cde470669343d27be9b0ab4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: scrolling.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/scrolling.js
MD5: 104c04ec259e68a53516216e4947e9b1
SHA1: 54446fd791e3331041e6e9a0874fa66d4794bcb4
SHA256:07f6964d12cb85a698967bcfeca73824a7b602475d488ed6f57e2981879e7487
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: scrollpastend.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/scroll/scrollpastend.js
MD5: 74be53ff23fb5eda7725c96f1ff683b2

SHA1: 1aec49fd4f7f5571fac13fddaad9eb1705cd522d
SHA256:6cd389df1da1ff9ba25728e03afb7f47df3162c3d9bdb5cedd06fc91c6199479
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: search.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/search/search.js
MD5: aee5a4efc34387df3d1974e09cd2965e
SHA1: aa36dc4a27460ccc0b4b40ee643907303b64a880
SHA256:4949580371fcd81c0ad70164b169dd8bcab2bd9869eddaa0d7e295508bec7a04
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: searchcursor.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/search/searchcursor.js
MD5: ca8612c41c44b87a10703ffe71d4f750
SHA1: 6bc4c36ea23ce7bf583f95ba4ad49e599bc646a1
SHA256:2c0b8cd8fe7ca5ca2253f4aacc914b390bff5b3cac3475df66c43a9ea8c8ccbe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: selection-pointer.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/selection/selection-pointer.js
MD5: 3ea743f9f1b458692e5258bcdc8afbd8
SHA1: 4306383d109eb987ee62a6e2defa8926dec870ba
SHA256:fdd7ff53d0ca796c5e3792ceb5063c84d0735bcaf198a1c06c78880f1c664a22
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: selection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/selection.js
MD5: 34d76a4a0d6602f8d4ff937e499f7906
SHA1: c759ce0c87a62abdd8916125e3bad601e4ce4efe
SHA256:ca2d26085ea9380b686c57d5ef8789e3c3032ed8c5d90ae0e1c9dba69635a89f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: selection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/selection.js
MD5: 8f89f30a603010383e7c118550697100
SHA1: da2d4548c10827c45fd625bdfd1ffdf0e28e0c30
SHA256:03cb03c86030e258ed013dc958cab854e2978893145cb096468ff8149417502f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: selection_updates.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/model/selection_updates.js
MD5: 252e2ea7a38323b8d82902e6595d23ae
SHA1: 27719d66e1ff98e650abbc5b48f2f4635f65df13
SHA256:a285a62ec8522c5d8271505b1438ddddaf39c3dbfd4dec5ac01971728e21a765
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: shell.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/shell/shell.js
MD5: ab0fc779b5fb9bdc1310a28d7dccd379
SHA1: ece7e7661886871cc46ef71248c67ea53a61ac7d
SHA256:24f77cb162ea9d9e9fc79b95ba547a7cc10a0767e3a5a52c786d4c24253736fe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: show-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/show-hint.js
MD5: 60b351da32481256f3800ebb7254245f
SHA1: ee89a290fdb95c87e4f3298c9ac62ff1fa385c56
SHA256:6d940e45a07c13abd1e872802ba20f91f809d4b583afcd58a8058e25c7f0cfce
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sieve.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/sieve/sieve.js
MD5: 88c6148d955c6542b3f10482b736e553

SHA1: 72627a945e27e3044717e5b8db378f3d776ad0fc
SHA256:c233866cf4990e2f28f11c96ecedc7e7dc465c19c5b445b30bdc037118f7b65d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: simple.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/mode/simple.js
MD5: 282f2d54ca2c7b60ab4bc0cd762b943d
SHA1: f08a5e5394568164edb85911dfc452f433bb2483
SHA256:400f49309b31197c0c4ec76519c93647b494ab80f59f96d7f051463e0aa37eb0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: simplescrollbars.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/scroll/simplescrollbars.js
MD5: 34d6903cded2822fb2261678e1a479cc
SHA1: 0707d27834fdde0fe2c32935af79d4575cf9f1ad
SHA256:62b48bff43436bfb8ecc5e3273e6047f0b934c1d873c81e863e13bb462d1e1ab
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: slim.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/slim/slim.js
MD5: 447874e5c5dd225949004c357d17ffe2
SHA1: 2cdc3263aa6d9766131d73157afbf05fc6767b50
SHA256:a8d555221c610512119f2107d58bb1c57d294cebc91f82638ea6e235286b5c15
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: smalltalk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/smalltalk/smalltalk.js
MD5: f6e7ef04f9f907a13604ea5b1938d3d7
SHA1: 57f009cf2b2147f14c530f697fdfbd3ac493e053
SHA256:9f649668162a61cfa6a3528dbe513d012162932c742c7b0696078bd2a6d3b190
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: smarty.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/smarty/smarty.js
MD5: 3ccd6f2129ee79c85ef96a8237f1de7a
SHA1: 5fc274f49b704c0a99e0f0b9030c90f56fc7c1f7
SHA256:9e95bcd71635efe200c3871c57cbb1c07edc1f8206d173f4552fd2dfbcf9e9af
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: solr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/solr/solr.js
MD5: df4ba46ed00e24c144deaef9a817d024
SHA1: c880da8431afd54034ae7fbfedb45d94966638b7
SHA256:17f16060f00cd932914722bf2cd1a01318c402503b62f3bd2bda09bab6b42b85
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: soy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/soy/soy.js
MD5: 1db8a99a573b2ab07cf30cc58da1bb2a
SHA1: 7c0a178caed0b849f140d0b21de6548a0355f9c1
SHA256:358a1861e92366d238eb240fd5d5cf8ea6f5fe219f389667d277031c0a1a47c5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: spans.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/line/spans.js
MD5: 52150a5a01dd7c56de003aa132f71e25
SHA1: 92cc8b4ab38a103a106f574c40d25d16e97d48eb
SHA256:719ad01e720518e7594a76ed4dc4904fecd7c495b12d87fc4599b40032975789
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sparql.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/sparql/sparql.js
MD5: cc62407661d4db81a7c77c01cd719007

SHA1: d4675ce0d6471dd82e6ff962975b02598fbcdaaa
SHA256:67da386492db5a215029f64cf31d008f5a60b389da8ed3cbabba1dd698427e8a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: spreadsheet.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/spreadsheet/spreadsheet.js
MD5: 370c01bed3c433131f942ef7e6f69187
SHA1: 94b3e4c80f954a378ab94f13068d879e9ab3394b
SHA256:0807dd557c55f5b6d8579c5c9019c5eddcda9c56ce559190e5f2985b156a00da
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sql-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/sql-hint.js
MD5: cb1d5a7d12011ecfedb83af8e4b00afc
SHA1: c97a3091e625ad43527bc861c589251ec2fe0457
SHA256:8723e07aa931aafc160404ec65f0cc05b9cb44198edb3d0e61efb5c3f83d202a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sql.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/sql/sql.js
MD5: 153675f40c7de23adb30ce3dd2a0a3ed
SHA1: 1302b12a26400851da1628452d10374f39d70b51
SHA256:d5edb6bd39caa6155cab6bcdeb380a29229264a8a26e5fddd21ca12f0ebf359f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: stex.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/stex/stex.js
MD5: c7ef8ac785ee813860cc414ea17dbf6d
SHA1: 3e46d97b4e694c7389cd0df4d13b914697d28c8f
SHA256:edc1f57c69920967a31defb66954aa29f5751fdb2f7ed8e52fa08978ff890e3b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: stylus.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/stylus/stylus.js
MD5: 7e6d36c0cc269b4e518bd48b9b6342d6
SHA1: ea339b15b178a1082a2acdadae82ef1f4a599f32
SHA256:85683adfef4f0129670fc2e5ee9148ad956213f5fa0c8dd05ac7970ad7f0b337
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: sublime.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/keymap/sublime.js
MD5: 1d7ea7f929183e76740bd9d98e9cac41
SHA1: 84a64b60b5802e86b0689ccfa95665339347f0c7
SHA256:1d532a67594845cb7163b090a06da9287b896944ab5f22df67f14e176bd434e5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: swift.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/swift/swift.js
MD5: 903f9bc460349546b9eb26858e8756c0
SHA1: cb2da62d408e283f01d19d41c0dbbffb3c0ff677
SHA256:8966adf30abf408c6c611e1fa9070a0515d22cdfda468867e54baeb581d6d6d4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: tcl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/tcl/tcl.js
MD5: 28a739b5550bd5ad13b47dbec84a9716
SHA1: 2ce8afb99f36fece39e1b3df7be02509f77b19ee
SHA256:98552bab94ce9adc9fcef5658da2965994a84e852c83098e94564884815b3026
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: tern.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/tern/tern.js
MD5: b9418efb9c0d90a3432dff86169fd293

SHA1: e4d1225e756d51fcb69c2f14ddce1b09fa2a23b7
SHA256:1ebb5ad38f72115c49865b5537fd9c77da506b7ed2be38bd310306af3c698e44
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: textile.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/textile/textile.js
MD5: d3923b19d37114a9e2a346c191c318e1
SHA1: 979b17e6363d63ac2d1b3a6854ba6196564fc5d4
SHA256:c121fcf3e641a7433b9e328c76aa0b1755aa4c0412e4f59a1d8d6ac24b36df06
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: tiddlywiki.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/tiddlywiki/tiddlywiki.js
MD5: 3e4fb7a08d9df5cbe9822cb1756bec86
SHA1: 84885a1cb7be096c19a3dfddd70252efcc83960e
SHA256:4b62acf34df4acb1a4bc1a2729edaf221583679761d35e0e9077883810fccbfe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: tiki.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/tiki/tiki.js
MD5: 6e4bd43879571d0fdfa79714f550a3bf
SHA1: 6fd2ece4b20160c1859f34cb245b173459c21163
SHA256:af92cd0858a99f3c5cacf240874db7eac2704a7b193a3cdfddfc5ba70382a293
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: toml.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/toml/toml.js
MD5: dc2ba16cf830b53759b71306e9473ed5
SHA1: 1a394f9f45c508febc270b7c0a1f72460fc897d9
SHA256:67bbbc2696788633071f2a2b8a1cf6ca4f4ac82213e3d85b7cd183d60b117679
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: tornado.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/tornado/tornado.js
MD5: f45c2ec37cc008dc5dbd5f9c077ba666
SHA1: 8b55c6a85279c8f7d6b3f539fa097fed877c16b9
SHA256:d006020d7d093cb4f5ed5088ed151d4c45417fe5ccde69d960eb82cfcb9e0ecc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: trailingspace.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/edit/trailingspace.js
MD5: 43599469275c2b662b7907971147c978
SHA1: de4d3ee3d32f01f94921b8b3944c7383da7ba970
SHA256:a0d2c0196d8f4991cd58f320498f7aece971e502e4811ecf58cb5af8e83007c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: troff.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/troff/troff.js
MD5: e7f5f0a2bf68a81f0f3e547ab5640627
SHA1: f59246b4ff5ce93afc87a4ed30a0cba0e6ba4775
SHA256:f7714fdc46774467c168e75fc36eca90e6df16e27afd0b608b882b2df769b8c3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ttcn-cfg.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/ttcn-cfg/ttcn-cfg.js
MD5: d847dacea4534ee2841f01f5ac419060
SHA1: 0df7a9b8f5e91e2ae8d5a8a02c99bf779e221743
SHA256:22983894e4a3794c9bcf396e7a4119efa5ea07a4f97e060e15f3c13ec2c1a01b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: ttcn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/ttcn/ttcn.js
MD5: f94e618b386e8bfd0ffa2252482e9c84

SHA1: a463a8817c26dcec47a7d006aa097dacf74b28d1
SHA256:10be6704eac48032ce00890bdfffa03d445aae18e3ef7bd74eb14a26e5867a28
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: turtle.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/turtle/turtle.js
MD5: f36ec21c639822b370b87c63415533f1
SHA1: 9b6341bdf7330b71a5959cde815241b6e7deaf05
SHA256:0f82b51ecc43b95e55a752f80f719f8a39b607697b86d3fa4523a5e8280d3520
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: twig.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/twig/twig.js
MD5: 09ab2491f1056e9d142e233dbc9dc1de
SHA1: 4cb5eb7c9bf77dce80f92f2498d83af92f3398b8
SHA256:72b6e091bbd6a7c6eb786db2591c1f6f59c7880ef224ce5365ed39ec786d583b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: update_display.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/update_display.js
MD5: 251310fe6b3354bf1a036b1e3cdb60a4
SHA1: 117a3b4c00f591170c25d2ab495f4d7295460aff
SHA256:1b595e7ff1d45387a8ddeeeb39336a8a1dc2c9c2d966558a2228256b2c6ba5a2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: update_line.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/update_line.js
MD5: b9b8f3c5e697e33d73d1044eaaa86dc9
SHA1: 4f7c764ac36b54c918f06b68129b8835b22b55f4
SHA256:5fafd013fc16591f0c978c6a4bacb3cf054d52f5051becd4325de8c21ba07f7d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: update_lines.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/update_lines.js
MD5: 622269804f4310f70196691cfbcabc31
SHA1: 680ae9b79ac669d60fc596424985b5d1677eeb96
SHA256:71d6ea8ca9a8e6502eafcaa7b18f569c7777304a6d3d914abac8b1a4ca112ebd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: utils.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/edit/utils.js
MD5: 4e9e033cb9daa0702d84b88dfcebae20
SHA1: 8e5257ed7b93a00cb5eccbf544d6a1043f2edac7
SHA256:06220f9e424434492b73e0aea65bebba1fe74fc3002f8b3672d1d0d3a445f20d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: utils_line.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/line/utils_line.js
MD5: 0f6f365b60c1688d8f0fcb8d57a9d9d4
SHA1: 574435cdc400815c829db19a67652b7077b00433
SHA256:a8b39ff57b6d43dfceda786380d6dacef7b1738a81fb6033e7573502501d4b6e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: vb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/vb/vb.js
MD5: fa430588a34292ebd66e33fa60217b4a
SHA1: a89cb1b315fbed1886d709d921ae95b216d89fc9
SHA256:e8f8e4496baed70b1e6ff44979382bad81b921b9570b7da1a377835e973f28f6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: vbscript.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/vbscript/vbscript.js
MD5: 2da61e304ec310d9291e372c53c6b06a

SHA1: 9c582c79ac9ef6d1c08850c180f988bf974aedb5
SHA256:77109e0c2218502dac03b5bc3b290cfe0b46ea00f4d267f3dc4378d9abe1bdc9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: velocity.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/velocity/velocity.js
MD5: be30a2a88271b692c85d7de9744f7c16
SHA1: d45880a6f5d3d4840ed1297d7b3f14ba4c9a4be7
SHA256:3c076c7bdb1e2d3d25bffa1a682556ae449f1545c3731935306333b5831aa951
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: verilog.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/verilog/verilog.js
MD5: a79b1a94e41866ba625c37e77a76ba16
SHA1: 4818788973bd3f66d3b9e14992710d96a7ec18d4
SHA256:ae7c58b13650019ca08760e04f3ece3315e889eb5aa849a34400f16542610eb1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: vhdl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/vhdl/vhdl.js
MD5: 4f804b6884d0d7c233a0acc15fdab384
SHA1: d30d775adce22818b6e3955fae1d653028abb5dc
SHA256:da078efdda01a1245fb8ed5a16cffeb0a51823e5917e3802457041dc48243539
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: view_tracking.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/display/view_tracking.js
MD5: a26525bd629440e84b02128d6eb323b4
SHA1: 2cb6103f9dad13f5ee416f272cc9f8f14084ffc6
SHA256:077f385b690f0c7af9976cb7b6d2b60a175f762753a77b3060a6db2686a5ee81
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: vim.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/keymap/vim.js
MD5: 3a5542b6dabf86e3983f29c5c5a184b6
SHA1: b8afaac94045745d4517c9635a5d0c1c266db7ca
SHA256:c8124370e0ba7e76d5cde3c18d257c5c99e5578d6505f0eeaab5c791673c40e8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: vue.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/vue/vue.js
MD5: 9e7dbdd0bcaee6279ed4e77f5ebc36ad
SHA1: dc5c50230fdd556f9c3530f781b7a2b16ad30a20
SHA256:8b9c4f59c1230c537f44f593f5d608a81604e4b3dfd345ea938939d0d62f668e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: wast.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/wast/wast.js
MD5: fb1f6ce81911f07db605e2e5ccf41cf2
SHA1: be86e08e18cc74130b483022c355846d72116c20
SHA256:8e8ae8ab4475c66d2f05960ffda597af6279c8c93f62cdab443407bea74c0091
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: webidl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/webidl/webidl.js
MD5: f31e84cde3fcc1fa2efec9889038d7e5
SHA1: 0757847217a95faf4defc9685f6821accb9d8988
SHA256:a12293542727a69514ae5477a65e33eed4f871fc207c6b275c9d8be1f2177062
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: widgets.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/src/measurement/widgets.js
MD5: 675098b5f0aea0bf351a1b5762febfa6

SHA1: c922dccdf98c79f92fa086bc2a36d970c76b56df
SHA256:09874ad13a856fad11b3afd084e58411741ee2735e61b4d95fefc060b60bfd65
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: worker.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/tern/worker.js
MD5: c6d16e68bc203e9489fbbd11b5b100ef
SHA1: f8adb9ac9944f88bf6e69048c001f89537f32198
SHA256:80c0e9bc4e2ef9ca9c97199818318429d26fae0d2452a20547b1e458eccf794d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: xml-fold.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/fold/xml-fold.js
MD5: bcfaae27958026e83cd442b5df731da4
SHA1: 7ad4740f2ecbaa3869b066156b19401075a0315f
SHA256:4ad0fdc2f93882174c9071e9a3c2324d15d4deb0c43fe607f9efe01dda1af9b4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: xml-hint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/hint/xml-hint.js
MD5: f2651770cad286ae58d12e9f5c4e9e6f
SHA1: 17bce6be75e45d7a291a32d0c1e346e4818296db
SHA256:6b78f04d2137358d5a01e9fa2b3a8f069acc70f925cc7efc39448ebe9599a805
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: xml.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/xml/xml.js
MD5: c93fe254ef100aeb5c9dfcda4c91d27f
SHA1: 510c71566cf81560cb5bd1bb25287ed6502dde75
SHA256:dc7e44d410399326f802e2924573cbf6f942a79f647fd0b97f0b607973bc9a09
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: xquery.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/xquery/xquery.js
MD5: 56cd9562591919c15b7610f13cd112be
SHA1: b294546669da04806196e6aca774914a30a0b3f8
SHA256:618685277efde78e0e48fd5cf95948ae32a4d57de942038ed0579415f3f2f9dc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: yacas.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/yacas/yacas.js
MD5: a70c01cdbd7d4311d4dda287ace27a79
SHA1: e853bda930d5fed1db0bd56ab9426612e759f9b3
SHA256:edab39fac054aaee5ea8ad3d09e0d38f57d5b24f826df7561526b5efb229fc72
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: yaml-frontmatter.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/yaml-frontmatter/yaml-frontmatter.js
MD5: c2dc6071833d8d9bf02d81244403cbd6
SHA1: 212780f18d78644233eb826c8c660eee51b6ac70
SHA256:98baa91eee7ba77aaf150a59d7e5146d4964ddb271076cd963cce43f9928b3f8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: yaml-lint.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/addon/lint/yaml-lint.js
MD5: 925332d44aefcb89b106d4fe9b32e93d
SHA1: 19221be874d11d57582a77dd08fd2f244e9b5500
SHA256:ee7249600f6b395c302b24054060f8abe87cbaa68a9f426593ca5e5f3748bbf9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: yaml.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/yaml/yaml.js
MD5: f0d36d2bba8f725438c8a6dcf5cc3b3b

SHA1: dfb4649752c3fc0251a05290b409aa420826e28a
SHA256:7de73109e5bfb6951d53764f5210f00f7859b57525811fab6b6f843980a7726e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: codemirror.jar: z80.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/codemirror.jar/META-INF/resources/webjars/codemirror/5.65.21/mode/z80/z80.js
MD5: 85b28ee5eafe8552bf842eeba91325f7
SHA1: 34971fc9b5ed5aa2f8714030186cd3e0056cb2ac
SHA256:0f501d7b8c9c48942900b4d7131f5bb18130395024e66ea5d98aea480f845e2e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar

Description:

WebJar for crypto-js

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar
MD5: e70e1fdbb3054453cd57ab3368e6bdb9
SHA1: 622835f605f708155af4ffdb1fda1fed2983bccf

SHA256:9e11775c13feb6a3161844db96974ad007dc36d1f4b3033555f34813a1584270
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	crypto-js	High
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	org.webjars.npm.crypto-js	Medium
Vendor	pom	artifactid	crypto-js	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	crypto-js	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	crypto-js	High
Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	crypto-js	Medium
Product	Manifest	bundle-symbolicname	org.webjars.npm.crypto-js	Medium
Product	pom	artifactid	crypto-js	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	crypto-js	High
Product	pom	url	https://www.webjars.org	Medium
Version	Manifest	Bundle-Version	4.2.0	High
Version	pom	version	4.2.0	Highest

Identifiers

- pkg:maven/org.webjars.npm/crypto-js@4.2.0 (*Confidence*:High)

remotegui.zip: crypto-js.jar: aes.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/aes.js
MD5: da81b91b1b57c279c29b3469649d9b86

SHA1: 5441866409bd32d32331c4b4b652057fb90bc298
SHA256:d6bb48feacbd63fd455becce7a5528877242f70e73ba1f7838c186ed8f35fd3c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: blowfish.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/blowfish.js
MD5: f324783486bb1c6c2bad1faf07c63372
SHA1: abce1a3fd40ce0c3f511fc0ea0be9a5d9006e580
SHA256:dce696d0842412093ec68ceef095d0db470a358628dbc352867bf535ef3edfb6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: cipher-core.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/cipher-core.js
MD5: b9c2f3c51e3ffe719444390f47c51627
SHA1: fb31443b26eb46eba12f324ff2c567d28e43c9c8
SHA256:1b3331c29f4a1e222ebf7d3b9bd3458a308c2a47fc5e6cccb93f7d2d5c57533d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: core.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/core.js
MD5: b55ae8027253d4d54c4f1ef3b6254646
SHA1: 06951bbea3ba1ca54de91f0feefc13fb62b66f38
SHA256:2638bdd7224472f801890636d42df16c144ca46c84229ef3087190d21f935daf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: crypto-js.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/crypto-js.js
MD5: 4b481d280be0331ef01b43c2d9b2a58c
SHA1: 4e84b6508f97c27e80a3fdeea2923d489d2b8fc5
SHA256:ee02257ffbaf0a9b481c7039b0f3bb20c360c9674fe4be8b38ae709b2ea59bbe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: enc-base64.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/enc-base64.js
MD5: f551ce1340a86e5edbfef4a6aefa798f
SHA1: 9e1b1bf75f35833ca2480ee401b4cff8b7eb1fe3
SHA256:84b69d1625474179d55622a8333c3aac376dd8bc77de7b06c21695762cb69cab
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: enc-base64url.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/enc-base64url.js
MD5: b87419e0e9ad776b37cfce5433ff5852
SHA1: 24aa5251bd4c6b8ca1bbaf0a5ab838fbdbfcb6ab
SHA256:8747798ddd53f467bebd7101bcd053b3f12ef028b3e6c012aede147732c8a9c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: enc-hex.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/enc-hex.js
MD5: efb02f85686d948c69ad13ec6a7d479c
SHA1: 27f6a54ae346ef0a9a63084990591e0f986bea38
SHA256:c7dad9931250921c24508ba9949abb818745b38891da44693359249b11ed143d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: enc-latin1.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/enc-latin1.js
MD5: a8c77d13f48479c2f76678c6e7f06ca8
SHA1: 9753af5959867f998f0feffd6f1699e88c92f39e
SHA256:24dfee2cc51ec0481aad1f62933bd0ae1238c34c5b0e73aeb1729027c913a26b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: enc-utf16.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/enc-utf16.js
MD5: e24e079fb22a2f7063cb9f856bdff10b

SHA1: 01f29539d0bc1e2c10638d0f3b9af99d978e15f7
SHA256:c35339900b45fa701c390c924009a95270b4b4d91b427e40984f117c2f7ec67d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: enc-utf8.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/enc-utf8.js
MD5: 5a9aaa6b97e87bf258edf26223bdcf61
SHA1: 16bab2dd76daec10b9b3e2569f3fc1a207b5f726
SHA256:8c7e44dc2d49b20fd78a44827fa962a28a5e22e0adfe036aa0fdcfc7adb89984
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: evpkdf.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/evpkdf.js
MD5: 7106e06bc97d1f59a9324ef5ef9c14c2
SHA1: 89cccca6c0e5261d31302cb4726a26f21a84ef39
SHA256:03a8ec00db105b3b813902400ed65169d12ecd382fa13402fd62c55e251caacc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: format-hex.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/format-hex.js
MD5: e2f78f02b844140cb8763fa7cd8daa45
SHA1: a359182575c8d43c6e5381209472f8954e4d5496
SHA256:040a2918bec8cb8ba0a6303fa3c1bbfd899bc8644643e8ac493e3c08a0c09097
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: format-openssl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/format-openssl.js
MD5: 502d6df5aa16084bf5abb0f3077c13b5
SHA1: 7507a0c1ccf7049a8a10bf2ed73f24af5ed00aa3
SHA256:1ffa86862e66b6c0fff35cb96875e97a793aaf86ca749b29381cbc67a0877bba
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-md5.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-md5.js
MD5: 95b2fb61fbadc00bb3dce9098e37256a
SHA1: 143d92d0c7d56bc57036c318cf78dc50cd72b557
SHA256:d3072014eb4186d02e335c511b3cc6e163a5cfebaa8c4ae13634af24887078e6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-ripemd160.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-ripemd160.js
MD5: 6d51886c1d976bc143c790593cdc0920
SHA1: 29a848612a72b95abd8d8a9ee8d4874939fac6f0
SHA256:28e2bdcb143840e4e01eff312a728e0f652d7dcb0d1bbdceab0bf48ff5cae8ac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-sha1.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-sha1.js
MD5: 4acf006c1688cf4513ed375d7a94f86e
SHA1: 8fbe2fbecb2caa64f74c0393f9f6641f78e3b732
SHA256:e104acb7379b834bd9249e3cfcb2196acbf90a22bb10947feb2a1fbe30ded105
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-sha224.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-sha224.js
MD5: 875a7a330903a92828b279818e6b06b8
SHA1: 586cc496e368eb6f6119e0a6089ef7f8f421dee6
SHA256:35208e1e4631ff5f9bd83220dbfbef63290eb93e914055b35583fbf19eb76693
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-sha256.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-sha256.js
MD5: 69817fc0da86033d4ef559f0febd3d32

SHA1: 84c60e2a1dce8f06c1e4340542199cc9cc9a3454
SHA256:11d26c11f858b74bf0f106c74ddb579a112d3e7321fd684365a77ba2a7a5dffc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-sha3.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-sha3.js
MD5: ea6cba03f7c6b257b70c1497022b5514
SHA1: 0d8f8002491a9311c7035aaf07d4a0329f38ced0
SHA256:bc63c36741416fb55fbbe3c7c4a78b5e056d9b902a471bb16b6f5672fbbacbf8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-sha384.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-sha384.js
MD5: 7afbdf157b81970eb00a50bc421e7ce1
SHA1: 9196d839c46163f6e51c63410ba0076a09ccf178
SHA256:93494b918b2eb79cd1be66145a41137ac0d65739ed6cb9e04f82bf1d7cdc7019
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac-sha512.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac-sha512.js
MD5: 5d3e9930daf490e45b446cb42b31833e
SHA1: 4b07089a6c56852d15ec948b58408d5b5d32cafd
SHA256:6c2b59ac5e27099986b28d32e425ed3d65a4621c1c6512d03d40b336c6e88a2d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: hmac.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/hmac.js
MD5: ee162ca0ed3b55dd9b2fe74a3464bb74
SHA1: d68f1ed4e3aed7807fe17a8193fca4775221dfa3
SHA256:c89f8f08ae06990edbc0763cd46853d16c70eaf513de8592b1ffb74a2ad2f7da
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/index.js
MD5: 8181544c4f4842cba38a939989ddb460
SHA1: b4ff6b82e1e72ccc2a5de8f94968c3b82060f61c
SHA256:7de6a6041ebd1a43ecd79b59708795ac273930bb36265b41fff832d781e7bb27
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: lib-typedarrays.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/lib-typedarrays.js
MD5: b8bac2e22a7a589167e014be77736c72
SHA1: 622fc0f297b3799ff91b08469989e6fe113cbda4
SHA256:a5875f287e6cc6dea0ab64024db32783229a7db55f74deccf6566973bbd76ec9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: md5.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/md5.js
MD5: fcd0c8cd3533c15bb4f0628f82cf5175
SHA1: ed91751fd5c6009667d6b43c5fd3939993edd568
SHA256:ffce8dc6b782620c6238a5b2280c5a98f6bef8c77fa80e581fac8cce0f08effe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: mode-cfb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/mode-cfb.js
MD5: 5847dafc1beecdcdfd23925f9f4989b2
SHA1: c9972596e02db6c6221ae019dcf1498d30e9ffb4
SHA256:a3626b78fe53d7d32fbcaeaeb92750db305e84e2ccb84e61d735ac7a4dc7345c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: mode-ctr-gladman.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/mode-ctr-gladman.js
MD5: c4bd3b4755cf275747f8e68b0eed7995

SHA1: cabbcc4100b4d363f1b55d42b930ec547ad67dd1
SHA256:fcd6166981435cc01bdfd2fb8f9e2773acfb144ab8c47e0c71473d9bdee755b0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: mode-ctr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/mode-ctr.js
MD5: 6cec0458e4e62c1ff8b534e59f9132ff
SHA1: 591484053ed26919fa6e4cecf7aa723dcade4bb6
SHA256:9e67161f61922a475b142b2e18cb4470ed7860ef61bc6e7a41f327f7a59be96f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: mode-ecb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/mode-ecb.js
MD5: 3a84195b8427195dd9c345a0f3aa2313
SHA1: fe621e95709e31a5289c78d114aad4a920f14923
SHA256:4f563373ba4af442e1b425b7b7dd1030ed84b9babe9821949922d9677bf14701
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: mode-ofb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/mode-ofb.js
MD5: 48f5529799d5eac8fa9f855ba1402737
SHA1: 4e97befa1e4d0003cd2fe9d21d85d6636513fdb4
SHA256:b49077bf4bf5e8f2cbb2de0e2d48c4d941a3feba2bc7c629abd51fe2ac8bdb2f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/package.json
MD5: 2f31b0aec8f5d1c63af62bf46623876c
SHA1: 7316c3382382dee4cc36236a13bf43543b8a855d
SHA256:011d61589c95ad4e16051c492565f7c19c6a7832580674503cceeca612e7a6cd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pad-ansix923.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pad-ansix923.js
MD5: ca8ab3266976ddad6e811577212b8c88
SHA1: 505018913484e110aa81842a4511a2a52cbf2231
SHA256:7d950bc42f262159a2786eea30d1153a3d0bca9aab9acdbcc1a981a8d2854ef7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pad-iso10126.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pad-iso10126.js
MD5: b1c4aa95c8bc79280076e66352b6c219
SHA1: 9c081665a8d0f4399c5f3874f38f811932900d54
SHA256:d3695304e8e7a001cc6e1b84d4b58abd429dd7e3f09514c260bcd3122a3aa685
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pad-iso97971.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pad-iso97971.js
MD5: 4027c92ac1ed3c95f39e8e2a391500d3
SHA1: b7034e19bcb012cf7549baea65a70d25b8e71480
SHA256:f7f7179b8bea5b6ef4f0891f23b563db8aa530376795cd99ef84942cfc62d328
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pad-nopadding.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pad-nopadding.js
MD5: e288e14e2cd299c3247120114e1178e6
SHA1: af4df0df185ab10e12fe8c01f885027eabe3c8f3
SHA256:a722d1f1486b807b34076ec3277ea3a65f21837db2d9f76eb5daa7de312479a6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pad-pkcs7.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pad-pkcs7.js
MD5: 23c101a5a832bfa8a894b9813323044c

SHA1: d21f12b724eccd65c9f20503bdac2c41eb8ce985
SHA256:9a3c909e8c3b6604bfd7a48a3c7e61504292744d894bce1266b44691b857c1bc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pad-zeropadding.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pad-zeropadding.js
MD5: 23b4116306620a01bed22b52014c7c65
SHA1: 34360c2d2f9a38e5c3d197223a2f5b6777cbc1e9
SHA256:d99e781985e817da7c6af30d957c45419b1a7e176bf52160424ebbbf970df906
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: pbkdf2.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/pbkdf2.js
MD5: 3f2876e100b991885f606065d1342984
SHA1: 006198366f41423a82b05dc582d9882530c3f6e5
SHA256:89cca1be3926c8d89b6f827d70970bb3bc94ae47943342ca8949992faf8d2b60
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: rabbit-legacy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/rabbit-legacy.js
MD5: 8fdb6b7d8bcf3aef27398d47d13dacb9
SHA1: 23dc78f4b418c296ffc166bbcad8c678d6ab2efa
SHA256:cf9afefa87b216dd4d8be00524f8904bba1147fbb90273e5e6a7b2824b52e56f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: rabbit.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/rabbit.js
MD5: b3bae9fc93314924cbd6c4283c1e91ef
SHA1: 4bd339e3a9e954c2766a07a96cf7ec2547e76cab
SHA256:dc93dba650db41783f8a3faba6ba17ad82cb0eb1b6fa84df406f71d520d84b42
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: rc4.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/rc4.js
MD5: 846a99f1e90dbcbb5773793c3fe8aa5c
SHA1: fbb684811bde18ce2faad2ffbda3aa9c00939e90
SHA256:571eca05c055a26c729f757f83b9f849968ae0dc0ba9870e5be9526019c53a33
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: ripemd160.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/ripemd160.js
MD5: 1d13fd2d4858d87c36c43a0a6436f0d4
SHA1: 9187ea140085390e357f1e7804f95e7a5812d494
SHA256:3d7eea732acb8f27ba7be5ec54cc1c5ea198be2f7b12ae78cf03ce3b87d78da1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: sha1.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/sha1.js
MD5: 5fbc23cf1d5cf34e9f7798650d07b333
SHA1: 7401e77dccaff4ecaab8e57fd11fccfaf5f33c75
SHA256:fca2d5560acb8de760ebc94679ff210056722af8193871e75176a61a977ac30f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: sha224.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/sha224.js
MD5: bd908518f276d2df58277bb38185b307
SHA1: b10b13e02fadeea29119f6976b346d9b06c84342
SHA256:542ddc722d9711595c11d57caa9424beca928b3553747a51e3f1c57c2c08ec16
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: sha256.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/sha256.js
MD5: 561d24c90633fb34c13537a330d12786

SHA1: 7593f14b59ba2099cbb4ffb806e75758fdeb12f5
SHA256:d8074f23cbd27aa6c2f231b8bdad34bbd8d49c7e47ffa0d7cd07a2c4d1d3c798
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: sha3.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/sha3.js
MD5: 6fe2614bbdfb802fa873f118621c7fb8
SHA1: d977f518e609149d1b51932648669a4be7a97f27
SHA256:6ee08cd3d69b181cb735011acd0a0d57b6a4a071baf8ecbbbb9aa18cf1e4d6ac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: sha384.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/sha384.js
MD5: 6ae085f20325eb927ff673ef20568137
SHA1: 8d7bb4a99b713d53723f8f1ad3442cf9e9edf9a4
SHA256:8d902216aef6840bb9951117bdd3aa6331078e68ee04987aa1d59c73b5ff3066
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: sha512.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/sha512.js
MD5: 0e5e8946947671eefe910c58f1272c48
SHA1: 7b4efa121b30865b12f7546f1e99e22c6c2a3c40
SHA256:986ca486a1c9e58e9d8fc38d1db4e652e14c751ba1a6a15fd81439d261efe2b0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: tripledes.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/tripledes.js
MD5: fcd80fd597ef5e6a0fe34cdf484a8825
SHA1: 94c5615ac7a0f2ee61bb5325e46d61151893dfa6
SHA256:8d8de06235e08f38ddc855070ef8cb86d7c69a67b3a5278f8cbf2af64b55122d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: crypto-js.jar: x64-core.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/crypto-js.jar/META-INF/resources/webjars/crypto-js/4.2.0/x64-core.js
MD5: 677577ca38d04508f116ebc977dcb11b
SHA1: 966f596f1adb7e7780021ae463a62890de8b19fc
SHA256:c54130dcd19ae2c7f8c4b4a69cb2038a65d363899cddf7ebaae0102bfc8fe086
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: echarts.jar

Description:

WebJar for echarts

License:

Apache-2.0

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/echarts.jar
MD5: ab9c65d2fb8370e360fbda0af3a90619
SHA1: 6d43401ff3db73afe10c16859d1e6cd88e43dc0f
SHA256:4a053ae22b38e441927603ed7b144924660e2ead54a8cb6db75bcc2b895ddff7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	echarts	High
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	org.webjars.npm.echarts	Medium

Vendor	pom	artifactid	echarts	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	echarts	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	echarts	High
Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	echarts	Medium
Product	Manifest	bundle-symbolicname	org.webjars.npm.echarts	Medium
Product	pom	artifactid	echarts	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	echarts	High
Product	pom	url	https://www.webjars.org	Medium
Version	Manifest	Bundle-Version	6.1.0	High
Version	pom	version	6.1.0	Highest

Identifiers

- pkg:maven/org.webjars.npm/echarts@6.1.0 (*Confidence*:High)

remotegui.zip: echarts.jar: echarts.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/echarts.jar/META-INF/resources/webjars/echarts/6.1.0/dist/echarts.min.js
MD5: 3772cd79ed4f608d0d00366c127545bc
SHA1: 1a87fe59156db88e222ea27eb2c07479d37b2db5
SHA256:b66b25aeb4df84e33199dc21694014d336d222cbd9deb0e5a7c14bd6aa0d0fd0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar
MD5: c9985319d244f7df278b01d7308df10c
SHA1: a304c306ddbe826ac79f7ce83ad9e8c0a0222a4e
SHA256:d2eb852d7120db344d837675afd1a4725104d7fc4dc4ab9d88c5f714128426b8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	hugerte-languages	High
Vendor	Manifest	url	https://www.tiny.cloud/get-tiny/language-packages/	Low
Vendor	pom	artifactid	hugerte-languages	Low
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	url	https://www.tiny.cloud/get-tiny/language-packages/	Highest
Product	file	name	hugerte-languages	High
Product	Manifest	url	https://www.tiny.cloud/get-tiny/language-packages/	Low
Product	pom	artifactid	hugerte-languages	Highest
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	url	https://www.tiny.cloud/get-tiny/language-packages/	Medium
Version	pom	version	1.0.10	Highest

Identifiers

- pkg:maven/org.webjars.npm/hugerte-languages@1.0.10 (*Confidence*:High)

remotegui.zip: hugerte-languages.jar: ar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ar.js
MD5: 823f9945c776bff8a5d1d33b7d053f76
SHA1: dc44a63c5afd84dc271d61e5673fc814e1de20f0
SHA256:16ea01e589d138a6136652e9bbbff6f0a78c7da2c52f777e50c2b1c51b85cf6d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ar_SA.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ar_SA.js
MD5: de0f31d1f1a0932c71125d7baef80a5a
SHA1: 29240f1954b11d0cc527d22342d62b23d6be35d7
SHA256:df5dea24dc375556b47d00f787af4457a306dce441d7560dc5708926e65196a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: az.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/az.js
MD5: 41a5444280dc4fed40bd7007a8734bd1
SHA1: ebff1c1e5fe696a05d5b025cf996239d07e5728a
SHA256:56722b025676cc2a88be8cb111e7d93a1cf5f076e25b57603c9ee34770eb1d21
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: be.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/be.js
MD5: a21eb5c6f25273f8bad1ed7d263c9bb2
SHA1: 029a79f496d18774c6e463c76bb351c5e36d745f
SHA256:38ac39070c67cc3dab2aa62cf3c67f6aae5de17412aadaa7f3a7f0fc07fe1f5f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: bg_BG.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/bg_BG.js
MD5: 801f9914266c7293a3235a7fb0ae7f3c
SHA1: e7a34a80a73fff9be96fb31dc8f0f9d1a3987c59
SHA256:251201625c9f4281c1c290631b000379b84305155f6e36387ff62c21ee8b45f0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: bn_BD.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/bn_BD.js
MD5: 220b63a6f7d42943f33d94ba67423a64
SHA1: 86740e376336efef54a75384cc7b08ba1dbb8224
SHA256:afcae81dc0d30507f943432518ba500a7fbb86b4e215643b400cdbd1b1ca219f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ca.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ca.js
MD5: d44f1cce804fcec692b814e203609991
SHA1: 1cf7f636e5e5b04322d9d339da3315384c58548a
SHA256:268e5bd32cafc47a21baae85aece4afd933ca25ec9f9ead891679987c64579d3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: cs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/cs.js
MD5: 79a288d0c7f661ca7f5e3107341e4c9f
SHA1: 9aee0c1dcba66150ddbb2648fa9a827633e94366
SHA256:a3f3b00c1079b33aa9ea1ecde5182c5f1e427931e6cf82e85271d5e8ed85a99c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: cy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/cy.js
MD5: aa66134f9a69db8bf5e37e9c00486dc4
SHA1: a8e3c6399e8efe5cc72a88bca7d9df33ac016a41
SHA256:7b39d495ecb2ea1eca56270c5591c17475756c9aee5f0178d7dda9fa41201f8b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: da.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources

/webjars/hugerte/langs/da.js
MD5: 86be98bf9b1a2028d498158c10d995f6
SHA1: 2a88c16d9f97f6fbd64841c4bc7953775aa7c98d
SHA256:5f26a49c249458207d87d14f4a13ea76f9dfe83aa3192d9519aa3564caa5b593
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: de.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/de.js
MD5: c2a71fc1e4286824de66f53bd7b82485
SHA1: 13afdd59bb4a7ed1d67154bf5b5e8fd4e74ecc31
SHA256:89ecb25e929cb079bd55d7747c46f8c767d0ae6a82d0b5f4b88ed9764d899db7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: el.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/el.js
MD5: 915f10cf164e849c6fcebadab64b00ef
SHA1: 9915d6d53f204fb3098db4fcc6984f3c7aacb5ac
SHA256:023ff4f96e5a56be54b8f5fe60b5dd437e7e0701452a1b2c3cccd9227b6dc35f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: eo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/eo.js
MD5: 8f0c327a379a1687bd1d79b356e0c6b9
SHA1: e8db0b00cf0948cc7912deffc721d91d55b8bed7
SHA256:97e596fdc130fae102a9199bc538546abc46f300728c0f51697391d57aa31e5f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: es.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/es.js
MD5: 033628b467ed06d308c9612dcd5bbdb5
SHA1: 09113c6d952a730226b8a1d12cd237b3899789e4
SHA256:dade4c15e9cf8d18119ca2fdf6482b3853f5b59cf0f970d089170daf767075f3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: es_MX.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/es_MX.js
MD5: 449d6aedeedbdbe6381c83d9a5769597
SHA1: 5998163f1a11b65a5e7a0ab9c9dce230fd413e76
SHA256:bb871036a74c5306485caf250a509025740ee01a01c7423004462fea3cc2be39
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: et.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/et.js
MD5: 091758942df0564e10bebe19a78d313f
SHA1: ff025e62b8c42678618820b34d7931c5786b1aea
SHA256:6cc07e99a6c3b8c624a76c01a1fa3808711fae8f1f1dc47d2b8080b7522e8223
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: eu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/eu.js
MD5: 1485b45393804c99c99314aebbdcc0e6
SHA1: a95f6eae92569b428b700fb12dbe489a0b71a4f5
SHA256:cc21d29d3cb923a4ff36015cbe7bd17dd7a64a5e72fc6ac872e4c945db16241b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: fa.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/fa.js
MD5: 0dc23c9242a62695e3cbeb9a2f78e139
SHA1: ef67cbd5dc74eab86408aa69634ae8e2067620d2
SHA256:22e7c7518a2bfad61e9fcbe065ecc02ab03fa8534322980bce9f99ebc63a73a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: fi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/fi.js
MD5: b7e0faf1d8fe236d9b2936d625a0fdb7

SHA1: 20be70760980449856bb658599c1330a5a8075af
SHA256:4917f9d328011a6ef7ab83ad444289f6f99f83b715427198ba361639dad96bb2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: fr_FR.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/fr_FR.js
MD5: dfa01543f5cf0741603c794997fb5d9b
SHA1: 635f1e92319d08246c041243dc9095d3c93e1f8b
SHA256:bcdfb2da8b8415d7127043dd30676369f9beaec15d3f632bd4c956bf9cd52598
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ga.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ga.js
MD5: 845b69d910adfa4628178f438a718482
SHA1: 4943d1679c82f7e96a9336d77cb0d2c3aab1fecf
SHA256:5958b2e476b049ab4baeedc79aba6df32354d77ab53d5d247031c770b1511651
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: gl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/gl.js
MD5: a795d0920b1380017ff30141839551e0
SHA1: f88dcdaa4f1ccc07c852f840f98e2152fef000dd
SHA256:71207713e3e7847c58b60968a99f4a78433badc4fe7e30b72dba09aeca4555c5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: he_IL.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/he_IL.js
MD5: f0c6393b918763fc15eee6d3e0c37466
SHA1: 9b1b2433bdf168dbaa699f013d91e7ea7604e892
SHA256:78083d15ce5a545d77b567697bbf442b183cb251db84479fc6b4170d61dfb246
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: hr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/hr.js
MD5: 2441d08f559cb16b4d43b9d5105b860f
SHA1: e0482438bc1ebbe8a1d0fa678fbea00ef712dbed
SHA256:ce558c44bad214031591a960166ad57e48a3df1829acaaa11f5de44e4b7bf991
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: hu_HU.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/hu_HU.js
MD5: 2911b3d257d0dc7f14333016a7473155
SHA1: 05f276655db6d33333857981a6810cb23c1e4c83
SHA256:57edd0020ed40bfa8c8bf17d3ce14d9ad3f55ceded462b4455ae9b01612a692d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: hy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/hy.js
MD5: 39fa7cf899184e065693c210effa166f
SHA1: c1a4ef7965155b0bfe0c94264af6dde949ffb079
SHA256:d917b7cfcb80a52e9a36f8b4bd7e234bf946fa052efd0cf3536bcb92cdf092aa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: id.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/id.js
MD5: ed414a75874cc8ff481bfadbb830ddb3
SHA1: cbca76c07a1123375eea910af43aeadd620e0308
SHA256:7c1fa631ca44d4e22f9c50b9891fbcca962e0220ef09aee6a40e75d5cdfd1cda
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: is_IS.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/is_IS.js
MD5: 9b77beb5d73d767a20f9023e43b95cde

SHA1: 89b10e76a8640b05c60235c2cd14f95fcecc5eee
SHA256:628c8dc10e2139d038274d9f0df5bc71f07dc761f94ebf2d6b16b26c1d492d81
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: it.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/it.js
MD5: 90e171ba4678a4ed19a31f0e440aee2e
SHA1: ce567152b20166647800c975e326ff77eb80b769
SHA256:b65405201879f02f69f991462a9874c1a3a3cd73789f120e4ce01e0e67ca0711
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ja.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ja.js
MD5: 9dc6598ea78c3171a5c79d12e9bd0d2b
SHA1: 4e7cb9da114814fe1bc798fc51cda71fcd0b38a6
SHA256:f8e09ab0e2d7b205a27ac040fe43756055e49247b706fa7ce3010507111eb2de
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ka_GE.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ka_GE.js
MD5: b23cbf69f2fa02f39ed9086f46d0a527
SHA1: 96a4216380b61acd215df2c2c62ec2cf27506e92
SHA256:60f5880d40ce0196356c7f8f1ccfa77284dfd4e528165e9da1a540570b0e587e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: kab.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/kab.js
MD5: 3b7ec13af25657f158d12387daaf5ba0
SHA1: 413a6adc6339cff29fc21c8a1ee9d713dd406d01
SHA256:fcbbc32ff3396f8720fa5384f168495f2046b3fa6a38a3415bc6349cbe01933d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: kk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/kk.js
MD5: bfc0aef232b63aadea153d6169b33886
SHA1: edb0a148549b2481162c47544d83a46c26522f1a
SHA256:3a0eae48e37986a44e71d7aeabcc9048de840262309cb13ca4642b6a8f4c9619
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ko_KR.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ko_KR.js
MD5: 3c1ae38527476e28004119b28e635254
SHA1: 179653599026e2ac4cb9b87c2ad7762b8c792dcd
SHA256:0ad35f07972e8121a88dcf1106a2f502b71998dbb485bd678fbb48adc8a6e3c9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ku.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ku.js
MD5: 031a3776060e93cd2fcc2a469982794e
SHA1: bde4d51b40929f76f5517c6381f02ef63beec9fb
SHA256:4c69b5c3c53f4f9069a26c409eae732e76316c1a39cb50e2b6296b9aee256f41
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: lt.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/lt.js
MD5: ae38ef0f7d831c5a2c0ebe933fd37040
SHA1: e2267f00cb816718ceec6b265d536f0eb41ea7ad
SHA256:a250c03862616afd2a73875e64c2ddd130c3bda5d565b744ec64e85bc6401cee
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: lv.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/lv.js
MD5: 5e9a34b9de6fb86881a0c116f445fcf0

SHA1: 9914a2be93fa142736794389a8ef160cc64a8ed3
SHA256:7068369f71f128d11f274aed093a35b649d6ffe0e33ec5b2cb56ecf5be1c4271
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: nb_NO.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/nb_NO.js
MD5: 2b23909699f576ef026ba5fb78ae31da
SHA1: cdbda59aa32791840f8d0428c7cffc54d722b63f
SHA256:e1ee0336aab8a84310f002fbfec4b7636ff074b5646c4552be7a8237593156bc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ne.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ne.js
MD5: 885af0f75b6673ac70ef74b275396b8f
SHA1: 5cbd5c46bad6c490f79dcfc6a53649cccca0f4b6
SHA256:35322c1614889e08dfc7c46a8998db16efcdfd4b03ddb32e3c9813084920728b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: nl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/nl.js
MD5: 0826a3893ffe0dcf835c41f022fa6736
SHA1: 0e3d08a78eb44a9c625d380a05c0995da54f9978
SHA256:42ca9cdc0c09b899c4c31bc9ad8ca252389ef50ad3f19ec09ea8160ca044b751
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: nl_BE.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/nl_BE.js
MD5: 81b7362a9af0bacb4f46de26b7258f98
SHA1: 7f4f768b30b547d50dc27670114f1e5bd5a9de2d
SHA256:53578716f41e51150f1ef17e05294fcc4a9c251a05f63c4f9886c650999caef4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: oc.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/oc.js
MD5: ad364ff6bfb912aaa60afcbe530eeb84
SHA1: 7178d959acb8e51067c6867dbc104d07c7a174ea
SHA256:3dc4b06e29d1d0f9e1337341da3cc6855505b4443dcc505e60c75f0e8cc9d3a9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: pl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/pl.js
MD5: 73c0a111949ba936650bbca9d70e7f2f
SHA1: e862ea235cff52a45837fd4b80f37e38b9933c47
SHA256:d8630e2cd3a9abe445ed7475635580ecfb02da50ccf4d3534b275d7bcd7d85bc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: pt_BR.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/pt_BR.js
MD5: 4025b9c06a52018128f87471d7536250
SHA1: dcfe2f7fe4ef9b75bd76fe24f6a29639d26484e7
SHA256:bcdfab8b8e078ea63af41e912bf9fda8fe5bbb10efccd2fb59b59809dcdb5223
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: pt_PT.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/pt_PT.js
MD5: 9591ec64028ef59a6d4eed3254f77364
SHA1: ed58d2d5a64a1dff28c1083d808405a5437c5971
SHA256:f4687f157cacb710fefe7a234c7513e9c842375dc628fb85e356d7734e649892
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ro.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ro.js
MD5: ee5452aead10357b0225b214dd94ba7f

SHA1: ae56e4a834e45614d4f26ddad0d7e0db61441f1d
SHA256:66ee1e952526d1200d4426df433d3c9342ae28c1f4784715b1e2436cc36bad64
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ru.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ru.js
MD5: 5f4a09edb41ca0d3656f0d5ce9058860
SHA1: e4aefa0eb5f9f75fd1ea15807021e0867d860b76
SHA256:cc26bc049ef33a17197075266eaabe26a01ad63c304b964efcfc5cee4ceb41cc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: sk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/sk.js
MD5: 46334ad086220eadf9a63d34c0f2c0a1
SHA1: 100e6a70a6f05d43ee711601895399b3cbb7921b
SHA256:ff3342881ae9ce3f99283c5bb2874d1222b526ac3636148415f40cddd808d90d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: sl_SI.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/sl_SI.js
MD5: bc7133a87c4c9d0bd8eaf59ef8c874ff
SHA1: 29c1685346e76a3bed36059a6bbea63058969879
SHA256:58b6ab701cf8f0ee76a6fd7300e265cede6102c9acf83ceba8d4cf4b00251ff7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: sq.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/sq.js
MD5: 861c26592664176acb3e275413859f28
SHA1: e5f0e123e4d250d2b6e1ff6ef50f4ea3d7b7aa7c
SHA256:9e266507d00b4e3d55af374d7097e74a66049541f761c93f2402ef941b50d2f6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: sr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/sr.js
MD5: 85a21c38605be1a745a8d91d7d0b650b
SHA1: b42391f82ad5765fa205c62f6c63d1e365690c2c
SHA256:94c18c230ab69fd848a72c3276c91037f7a803859438d69b890395b97e9f1ff0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: sv_SE.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/sv_SE.js
MD5: 5ed724e831b0b24b153d2ee7db5b3816
SHA1: f729969fcdbb302547cab963d560acb8da35c1c4
SHA256:1ff7f0f713beb4d59fc3a45704ee9064264eba748dee158024af49ddd7d4ae20
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ta.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ta.js
MD5: e2088db6edf402bc276bfc8d6856e2d2
SHA1: 42f8f57987cc20025703e0ba4df401d0cc8511b8
SHA256:2704c32a0eae180c20586f7b3ac7a5d83e777f5d2abe14ce8cab8cf786dc7d1a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: tg.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/tg.js
MD5: cdd2d5743671715d8aaff1bda4ad1f94
SHA1: 917638fd2950dd42fef4dbf6627cf078bd2b7aed
SHA256:1ec107508768200fe55d3c56ca19f91bbcde436ae90d32c62d912f9131064038
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: th_TH.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/th_TH.js
MD5: 75f892fe79cac886b58ba8263b9304ab

SHA1: ced62928d872f509b9112a7be0bd652a028b12b7
SHA256:f09ba8c508eeb7fd2bd0a31ddb0909cde3e701a0c15a7f5dd7caa1aad1b721f2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: tr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/tr.js
MD5: 705bd62d8012d72d0d4911d3ff5630cf
SHA1: 8d3beb46e6610edf2f362b5fd52cf6aa8763a3b2
SHA256:96dd1e00efec4becd581735af1d6b1467cc9798de54f2e945ece2afb70d43e4c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: ug.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/ug.js
MD5: aaec10538e96e70ff869484f6c747c5e
SHA1: e398b581d4d74426689508a414eea025392e6fe8
SHA256:6fcda2bec399a07ae3684fdd4497318ed005eadf33b3ac24ecba3f258007dc0c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: uk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/uk.js
MD5: 99020cb723ec0b122e56170b40053d20
SHA1: 5fab28c63533fd3e3fe00d38cd63ba6f23c32b2d
SHA256:6f3fcb3f5f2d4920b3c5be68509ab140f28c454595cb5cfc3ad02e996146830b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: uz.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/uz.js
MD5: 6efa9afc8b45dcb30d5c20dc2d651a99
SHA1: 4cbfda4fa00dcfef02d859a683f6a2e049a395e4
SHA256:b03c325f76d34d3d62a0de7aed705b4c015c5cef8fe07aa10e28b5261397cd4b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: vi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/vi.js
MD5: 181808a7542470b9901cefad7eb4b5bf
SHA1: be4a2aebc0c2e9fe45f2fbe7e9c19ee5ed78d6f9
SHA256:24622b29a7ad643866d6c8a74277e58f207366f2f3c34b4311b42f93204092c7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: zh_CN.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/zh_CN.js
MD5: 7584b32dc413a2d39e5b85d9dafa173a
SHA1: 10dd91679dffb2a3160f40ad3188db117b9afa2f
SHA256:9c06f952379981963600a4b3aa40af35eec78c163d3daa9da681107f8c647089
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: zh_HK.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/zh_HK.js
MD5: 1b4894b4e6c2e724475ea8c701568734
SHA1: 552f1316a1cfc565a018ea4fab9129a3825dd6d3
SHA256:ba7fde91f1a45dd5c6901368d6dd18c24683a876629c54b88396222b493c4513
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: zh_MO.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/zh_MO.js
MD5: 90d19ed9a0ebb0b0680ba6ba483804eb
SHA1: 4912da322d65705edd33e0570e81714a7209020c
SHA256:395ffcd48bad59534174877050ef1f016fc7598382e46e6f2105a44620bcff31
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: zh_SG.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/zh_SG.js
MD5: e29a6f7769ede1bbbb5f96a5eeb2f24e

SHA1: 3407630e6f9c9919f5e7b4d9b74cc652946189b2
SHA256:0d13680b26585e33a31f21153391e341ff5d2c6a0803cb882a621e7dc5231284
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte-languages.jar: zh_TW.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte-languages.jar/META-INF/resources/webjars/hugerte/langs/zh_TW.js
MD5: 0a3c9f75e226b3129e8b7f89f7130007
SHA1: c940597951e8d42bafd5602b1801c00fccb1dc47
SHA256:1dd655d41c2ac0bd1e939d787cb4baaf427fcdec6ba22c0f612f765195d548b0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar

Description:

WebJar for hugerte

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar
MD5: ff9889463260557deb96ce1393767ab1
SHA1: 7467c3eeecf4563268d3412599d8c78de68d9346

SHA256:1e6652c85819e641af08663c8f05ad17784c4aa9a891e031af82ba8fb5731a8a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	hugerte	High
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	org.webjars.npm.hugerte	Medium
Vendor	pom	artifactid	hugerte	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	hugerte	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	hugerte	High
Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	hugerte	Medium
Product	Manifest	bundle-symbolicname	org.webjars.npm.hugerte	Medium
Product	pom	artifactid	hugerte	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	hugerte	High
Product	pom	url	https://www.webjars.org	Medium
Version	Manifest	Bundle-Version	1.0.12	High
Version	pom	version	1.0.12	Highest

Identifiers

- pkg:maven/org.webjars.npm/hugerte@1.0.12 (*Confidence*:High)

remotegui.zip: hugerte.jar: ar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ar.js
MD5: f5f0b4553a42a7a74e7be718fc557e2b

SHA1: 302dcb720a73fd97345627a102ef162125fee945
SHA256:9866698a529f686db8b4222bdeb175003c3e09c142ba130aed9fa98d5aeef08c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: bg_BG.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/bg_BG.js
MD5: e532c81c8e86f9066729809870cff6fc
SHA1: 4e1e104ee689097ff1192decfe90175300e6baf2
SHA256:b884906123ab5b8b1ca1ea4c156a2d6635dc42319b10cf51b4d6e544c8c56867
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: ca.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ca.js
MD5: abf90dbb77512d6a2bafa26c36c9e068
SHA1: 77120a22296fdd4c779f3736396215ad82276065
SHA256:1f8935be80e07f8b30a9a96f5ba621ecc2f568fc96f69614ab4e073b6b3eeafc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.inline.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5-dark/content.inline.js
MD5: a8531e7d906f77df4085d9ded150c281
SHA1: b255e033e1b16c6df35859cc23c49a33c3baad8b
SHA256:7512a420bf16d072edbd796eadc03c74483fe6f5947bb070f517a012b80fc576
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.inline.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5/content.inline.js
MD5: cbf28002f872e95b1e9310dec7df4bdf
SHA1: 22b3e10eb6a88534c75b1dc9be9d6b511eb53e08
SHA256:8d35969f2fee55d8d2eb61f1aa8a2372dd941c9629379dda6f9f131457132c03
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.inline.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide-dark/content.inline.js
MD5: ac1812f6eb6c6bb8e98918582d3e855a
SHA1: 4681a3ada53a664e69ee64477e735aa371cb5a2f
SHA256:f5433e2fcd731cc793e3c59313f39aecc22aa87dbc0a6b63ed1640ca6961dcf0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.inline.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide/content.inline.js
MD5: 3b6064b7d2242fcadf7c3cd1025eb192
SHA1: 6e92f0f2c271bdeae04920ed292d5385cc91d344
SHA256:ee579e0bb81106269b705dd351fd986dd576b01e418c5d7a9f34a15116163a3a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/content/dark/content.js
MD5: 12a33a74969f00d72c1ca91f5dd68574
SHA1: 5cb32c25b4cff8ada2bacd1591433e2024d6721e
SHA256:fe95484ed2333699b3cab62ddbaca86356602f5484995f45ef5fc19f8ffc8212
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/content/default/content.js
MD5: 164e8ab6b6dd273fe68514d2669afdfb
SHA1: 7a8f735e76b1fe76538f37adf6c84ddd6eb29da4
SHA256:96c7468b51915ccfc6e8666aebfe471a529bbfa31e4aecbb6ccd0b42d4b9b79b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/content/document/content.js
MD5: 849a3cca327ddebaeff5c3423a9a95f1

SHA1: d158579accdba911860d31b1fcef6290a2ec0b5d
SHA256:081d92a90af447d22c65a22c9cddff70280b984027bdba43f58d1e8e2116eb25
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/content/hugerte-5-dark/content.js
MD5: 2c3c36865a247499e54470abeb5a1272
SHA1: 1520b5e03b91a4a762825c88ef4589bf7ee704a9
SHA256:ca33f6043e7cd3ee1f26c5b252eb108be66b37ebc038efefe5acd83e3f9ce734
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/content/hugerte-5/content.js
MD5: 1130965418bf44c6d085f938cdff6650
SHA1: c59de9f12455d9eddfc658b74c28a355f68319db
SHA256:cec00ecbc3b3d3f8afe4586a97d23cb761994002a224c21be3e29057636013a3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/content/writer/content.js
MD5: e285a71ada5ae779e20880da9289413b
SHA1: 4ab15a7db114d8f543fb7417d69027d2b41dc29d
SHA256:63bd0b941741ad44a63494f4769e928e6a05c44f3f8740edf6a271695a78f926
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5-dark/content.js
MD5: 869b2478cd1cb26e4261f32396805ebe
SHA1: 554b32151dbff01c1b584173ca359ce0115c6a10
SHA256:1e2311e53d5b6381ff5060382d7fef7f551690610af787744c8a49e2af78b009
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5/content.js
MD5: 9d85292a93c6d2940a80f50d1f0e6966
SHA1: 935d111369099d41bd50a3db11d6563051a634c0
SHA256:aee448e5c016b1143a15ecdee0f43e555f3c9add2bca6af40cc4b36b88cdc588
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide-dark/content.js
MD5: 27e32e6a26eaf951122af882c050bc46
SHA1: e2dfa84563a89ba71b07a278f325e6c926ef931d
SHA256:752ec72540796afb108784a0db126e280634822ba36910d37d68c2f606f86d1e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: content.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide/content.js
MD5: 76c08495990d174584d15c5f50a8e5c7
SHA1: e75376adbaa0ac5d81908ec178263ada61dada8b
SHA256:23e53a768bc59564bcf0e8600b187a8fc8822e23c2f175701d760cf5153760a3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: cs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/cs.js
MD5: 1779aef97fccc89fa4e8c6ae639bec3b
SHA1: 0c798783fa338bcf0b607e19b69a157e5aaf67fd
SHA256:dfaf6a6afa02f7a7da5c27cde37b1074e860982c75ca4a7d8df9a42e8f1ad723
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: da.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/da.js
MD5: e3bcef539406efdba466a679cd9625ba

SHA1: 3529f5c2cb29ac9eb0ef88d41ca2007e5b78fac7
SHA256:96e1ded7bd90160f1a26e3b4e04128d0c45940c459cc25763a4898d4731e72cc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: de.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/de.js
MD5: 24268690ce3e0719f04f4d8bc47c1145
SHA1: 57d8098db012b33e240b5816d014960db2d80087
SHA256:f2f2eee6eb358dedbce018731c82def4a43e8343ce331fba26150f7377ebb410
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: el.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/el.js
MD5: 1f775a05597f190dddcbe67b14d4bfaa
SHA1: ab9abb40af9aebdd589aeed4b24f3c50771f9d9c
SHA256:f252b51d126cf0ffd18c3c2c68554e4026adcd0c520b1338ae353a0849178450
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: emojiimages.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/js/emojiimages.js
MD5: ed66bd2151af667299e6c60554f9e4ac
SHA1: ea6bc36f8302e15f1aae686a19816f76794bc2a0
SHA256:a8d5510fcb0f8e4f45deefdcf8b6ed12e343674f9e18c236ce7fa45e072aa27f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: emojiimages.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/js/emojiimages.min.js
MD5: 00945ee808286ac74239c311ca723088
SHA1: d3c2508585c67052a1809a6800fb645d1870afc6
SHA256:750ba3f27289d888b1899310950a9188568bddce16352a0244c1c0242e41a55e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: emojis.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/js/emojis.js
MD5: 8f5b6dad1f50c9b70bd807f6cabb189b
SHA1: 13772cdbfa94f41d84ffc1d87c72016576a9d313
SHA256:aacc15ae1a59e7d6d8bde23d5f105654201882b0a86fa9a8e689b1cdc8452784
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: emojis.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/js/emojis.min.js
MD5: b77fd0dfa98dcc0be8192bf7f7bb9a9f
SHA1: 137d76ba6858d7685f7128ff9173a19902110b5c
SHA256:fc519f30e6cb48e46eb4d8f9ed5cf6c1e4877e625c68eae31e7723e42ff53ae9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: en.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/en.js
MD5: 6282ec2e9f83d1acefa2850555212877
SHA1: 853f9a0d2a2191756fed83005fdea7f97b5e41d5
SHA256:2223298388692bcc135105122d1686322188e6511163860453d791d1243279bc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: es.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/es.js
MD5: 810a9870708a49348955ead70c5d7009
SHA1: c6e78b5abb4c3cf4d67da9ff7c848caf24861c16
SHA256:dbc1fb0acc05dd8e01e2834f69f5f19fadba93b90e76854063663e5b335fdc3f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: eu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/eu.js
MD5: 0d85c3a9cf44223833af08ff51d80e27

SHA1: 2ac31465284e8e4583a8ce69abb64c3ff461114f
SHA256:5f6c854cf8372351ab402d7fe1f66a5a837c08e979b8072d16f32166edc07b02
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: fa.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/fa.js
MD5: a6809dbb54bf58699540c6a210e3cfde
SHA1: e3c03f38d4b4da86c3e9eb761c9f1a1ed542f436
SHA256:6c4c3e12ef9d008f12fa5b603658a6a00a0940ca7e85048d87ef80666eb3c36d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: fi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/fi.js
MD5: b7f976710075bdcbf5e57ee57acb59b0
SHA1: 8a4b373ecc42055da226c1c31ad9d976a10b9a11
SHA256:e67af5c13c21f4421bf7160bd19aab9318e6d19955111c5b9f890a362d0899e6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: fr_FR.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/fr_FR.js
MD5: d2eb59e6f3de25ac913be0e61a05591c
SHA1: 715dfb82a6e641415c0047f2901b7926ee8179f2
SHA256:5005b632badb0fc86ceaa196753a4712b1dd76d50b79e0d5d6410efa96f55ebe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: he_IL.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/he_IL.js
MD5: 57b3dcbaeca69401b1a80d78ddb7d495
SHA1: 95b7e01187222aaf1ea80d0b74f846cc9a4f4764
SHA256:692233e8906b51c91d1d70882a0502be5dddb2027b5095c07d79c491925ad8fc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: hi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/hi.js
MD5: 9eea865c5a377f40de2f8b4c41da17a1
SHA1: ddd56f4bd89abe1c502e0a9ead4b913fb1ea00fc
SHA256:9585fc860ca2b1a749f458be9832932118b54d5e2b9591df62191ffa22102592
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: hr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/hr.js
MD5: 3279eb68d7116c5e50c2445e392e313f
SHA1: 2b3cb7b1e01fdd84b9a52becf9f310329f4bc61a
SHA256:93300531f9cdd8b934d7a2f421fa0fd36ac20b2eb7f09a0b25ae96b28c3cfd84
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: hu_HU.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/hu_HU.js
MD5: 27b9bf10dbe7c9c15b8ea20a44b569aa
SHA1: ca2dddca3514deeadbb45a59877a5498ecb7faea
SHA256:9d62a3922fb0f24d96143e1a677211fec156bcd53ef0f60b386b8738861efce1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: hugerte.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/hugerte.js
MD5: 608a51d79e72dadae4f71c988978a748
SHA1: f77dd4688fa469741ece9b55f30c07510c83ab1a
SHA256:9a84cb746a8c0fdd5c857adb90bb4ab0a769335a81246d69224df2decb1bb24b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Identifiers

- pkg:javascript/DOMPurify@3.4.11 (*Confidence*:Highest)

remotegui.zip: hugerte.jar: hugerte.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/hugerte.min.js
MD5: 4f869562fbf4bb6f160fb4bf6ec6599f
SHA1: a86e8883ad71949b770498c57966f60ea42518f7
SHA256:be8e43ec41c91e98897e19594c67eeb98fbe269a67cdab2cfb8cb79d298ff05c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Identifiers

- pkg:javascript/DOMPurify@3.4.11 (*Confidence*:Highest)

remotegui.zip: hugerte.jar: icons.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/icons/default/icons.js
MD5: 946e6ff563681f2a84bf542c7d1f835b
SHA1: 57dd9db9f500ae6bbc16c1b39d6871be228c12ec
SHA256:a70cbbbb7c397786fb814a416f691b2d39bbc1856af4c975acaccb27f190bb1e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: icons.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars

/hugerte/1.0.12/icons/default/icons.min.js
MD5: ee63c9a58bfadec7d3f124f01fe865d8
SHA1: 04bcdc2f358ef5f562ff3bf05ded0e86ee39fb1f
SHA256:c422b0ee2a8c7c988d377c3455b95fe98b95b07616de53abe547a631cb7845ed
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: id.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/id.js
MD5: 559f08d3791f170b18fab02235ec1682
SHA1: 3e1621e3d7f2cc26ec7c76e3aad8b10740284c1c
SHA256:6b6f28465d15233f2f9d98dfea0ba7e43d983f7c5a616b5cf26185ece8248810
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/icons/default/index.js
MD5: 712c532c3b060cd5981af00496091812
SHA1: 1f0e1f66069455601e60b07941f412ec8da948d5
SHA256:01dcd2e841efaea732b35abab85f9b9c177708377e8a71cca9aa1cbc08ce50fb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/models/dom/index.js
MD5: bf6538ccd91ff0c8c459ea52568dad68
SHA1: 039492d60bc08eff76200837b005f238a4a4d93b
SHA256:7e00163f1579c2463df0e1794c7083972c531e65e97e79cc1d3fa5fb79b8e782
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/accordion/index.js
MD5: 275d42a50d44665e7c641933489d2fb4
SHA1: 4fe5780ee870d8e4ed3e19b06a6dcba0745951dc
SHA256:cfcb10117bda3513b6a8d5fc147c46d599d939188819b053cfe8b037d27aab68
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/advlist/index.js
MD5: bf1fd55a8b6b4c1288234708e4a63e04
SHA1: 4c00e9817344c41649c8a5692b8a50f46e86ec63
SHA256:65afd673d4ccdd16025bbea20476e1e97173e975c6907b17a03bbbf3bfdb8e4f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/anchor/index.js
MD5: f53211f88e234e0b071178c50bb17158
SHA1: 7ce22ad1179e09599e011a9117e17a2b648fd131
SHA256:db1389e04f95143a547eac5a86b8b83ffacae1baa4abae7b1b9c71158745a10e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autolink/index.js
MD5: e71fe17e37cc448ee08c8073edbd8511
SHA1: 8f90089dd67c4dd2c43ce5bd0c2041957b33814b
SHA256:a8464397c27fa3fc75c53ab84f63daae3c85d7b25106af78b2337752f1e18768
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autoresize/index.js
MD5: 6f84b0950a44436492f038d3aa0ba3e7
SHA1: 4f4bfdbe1b26fa78144a693b7c3dbc4d33f0db94
SHA256:171a9ea14e7b62d3300d5e5d557bd55d366d3ae3a707273898df479c096276eb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autosave/index.js
MD5: 08ef53866b246c81dfe6ef294869a901

SHA1: 431a34505e18811756e55c896308c5b1216fd994
SHA256:421e960cdc5dfa2ed55fabf2223966e7b8ba0fa29b04eb16cd0d1076013e54b0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/charmap/index.js
MD5: 4c65bd74732eab0ab7e847ecba83b2b8
SHA1: 39b4ed0edd6e1ee5c4636b947e518cd4d07b1c22
SHA256:74c2ee3ce6dae9ab7052f10c47839820e2b8d15a8d82360d76c22adf2e140036
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/code/index.js
MD5: b44ce9c633a47f29ece07d74747d1e06
SHA1: 7ba540f71aa2a39348361b231a3836e247070e84
SHA256:989a665058a05fa887eae0f403aee3207efe08c27adbf298db424ddd877002fe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/codesample/index.js
MD5: 90f716db1597b13e7574913db0271635
SHA1: c27fea0504a61d12e50a8064c3c8f76993e57304
SHA256:090fd58bf0e341f935b41011fe6d785674f550720bc4d3d7fbe61b9d7250b573
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/directionality/index.js
MD5: f40440b25858539de61515b1dea80954
SHA1: 33d1633c7f24beec0f6d23c6248f0df20a16816e
SHA256:bacf651ffcb58e57f22f8f6fb14ffbf696a50ea7b868a1f4af9cd03bd13b3884
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/index.js
MD5: 9c2896100b43bf842537b98ccb1696bd
SHA1: 8a5d6682c000d686462ad08266489d5ef6e4bf6d
SHA256:f6ab4d39b9c01bdb42e11a9aeed2f28e173155d1a8c3744ae766db3820ab6b02
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/fullscreen/index.js
MD5: e187f0117b672a2e8033678f08d2f1f1
SHA1: d303bb5448dc1e0d404f366f07b51cd3f0487c28
SHA256:ea62f70b60de9fca52f2d2fa328391a3bf5d3de2965d40549fd1dbdd74f69d4b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/index.js
MD5: b5bffc3c2adee9b308f33253c4fe7004
SHA1: b6307cda1e5123ee6c213d4f2c072011c69876c3
SHA256:9740f6f6ad80924540a5bbf0c2a63cc9dfd8e61794fab7fd0f1b01a25cd6b92f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/image/index.js
MD5: 095a51c136955dcc74a7e0fd9604e21a
SHA1: e68b5998a5cb615262e6d82f2e823bed40228967
SHA256:c4680d28a23819fd558d0535d085e7362d8cbac560044be6c9236708ee8ccf2f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/importcss/index.js
MD5: 5e5f8c0aecc68703ecbbb0e4234e7d27

SHA1: 523289fb23e7e4902a037c16885ee32d836f00ac
SHA256:81545fe205f290c3c31c7bfdb4ba83b3081f90ddfccea856d4b6c29ce6944745
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/insertdatetime/index.js
MD5: d8a0567abeb81a32ae97c146b2056f1c
SHA1: 6178edb15029bf8995370971585639e047345aab
SHA256:f5e4e03c4fceeaa5e024fd441d21be9d6f403c124335e0f4430f3cfb6ec4d124
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/link/index.js
MD5: 77e9b56d47087efd55f769120600d9e8
SHA1: 75dd165d3fc4f04daa39c21f2ade96fdea9afddd
SHA256:320914e928c5be2837bec40ed93b5b6c536c027e67bdffd9db2119461057b7bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/lists/index.js
MD5: 024e229dcff4a27cfcc170a5410b4843
SHA1: 4c554e5bc1d9621a491410c001775da57f879798
SHA256:7790a64cb53b91a9153c1b69bc3da83e3b159d20a7af6bdc13d27874a4615168
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/media/index.js
MD5: a1da1bf87b3ac65830fd803e9a28c381
SHA1: f09ec4275e63ebd377840fad37a65b011ddc6631
SHA256:45426a57dc58b349746fec58e3051f139895fdbd818c671f8f7c17443c46b701
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/nonbreaking/index.js
MD5: 8c1c718293b28a845a15c257772ff932
SHA1: 7fa2acf1e9f7bc30632d71735ef9ed0d2f9fab29
SHA256:720b764ae93c6103550a9200e0effd11853b564f2d6be45743bd17e4276a23a2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/pagebreak/index.js
MD5: 165034455e178e0eb99918d3a1421dfa
SHA1: 8af3f0527d7530ef2e63e621e7dea1c3c376162f
SHA256:fff3b308b4a7e7e6756f7c1cd80517f788c8fc0e95cb9b7bb360b6f24892f5f2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/preview/index.js
MD5: 83bb991d584186dab916e348799e4e2c
SHA1: 263f51c7a0512a1bed20eff7895b6498978532d8
SHA256:2e7cbeb72f62c23c850b1376295742a5c4908ce80808e8a9b9de214deeb7a72b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/quickbars/index.js
MD5: 99532be871de2c1e018b2f38fae3f505
SHA1: 4dad183c0694e2b520d32253e332e10179891435
SHA256:3b0f4ee52d5f152c733aa21e443ddb633517fce8675fdb8b164346e32cea3770
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/save/index.js
MD5: 358e82db36264f8bf5d5f211581d2e12

SHA1: 85b2560fe9b4c7dd77be693082e8ca54561d04e2
SHA256:e4ad55ebe0c5dd257c742be63db9f7faa361a03febcdb6949b34e50a5958e257
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/searchreplace/index.js
MD5: ed22a1e468fc1241e3e70c8720098442
SHA1: 49ad5ecf24b66612a3e9e8f1258f5fd8d1ac6624
SHA256:2e9e32ea2edcd011f669cac3b7bf65efd4635a2c24c72a81167a7bf79e6a4c73
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/table/index.js
MD5: a40ed84889ba858c1d78a423a7339067
SHA1: cea53ea715d6b6010912a3bbcec73e7c9501bd4d
SHA256:e23ef84ba7634338aa304fce140296fb95ed92bddfa40e1e8975a2f725de0dc3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/template/index.js
MD5: aeb80b7c4b07610c34901a284b372ed9
SHA1: cccdcf94dd46b6ebfff271867bace1d0df8c3255
SHA256:6b6206bca3f79af4262b418278b2b1d44ffbf0c16e618d6daabc3d022e555d6b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/visualblocks/index.js
MD5: 99fbe6ec0ba267d5bd4f4b56834bd6df
SHA1: dee26e00314addaf5d7359e4f672c6fdb309b17e
SHA256:1527138d82593c7a2c56998be7d938c05b1d18dc01590ba8638033f41655dfdf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/visualchars/index.js
MD5: cc4e861499e09f90d3d9214c307a9078
SHA1: 058e9ea96642f6d7da84f762a854c9aea27c7a5c
SHA256:09730d585920b1cb562c8e382cb7180101b81d419930364aee24714e1eec37fa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/wordcount/index.js
MD5: 042a01800558e0b5f08e835cabe311ee
SHA1: c0efda748192eb1ec1bed53d5d48447899f9e7e1
SHA256:01e372ddddf4f6441849ee78e1ded584ebd68d35fa0a7da3abb7c27fee75b90b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/index.js
MD5: c116e3f9ad1e1e3e232e65a88c76606d
SHA1: 4b21b67afb114f7d741f0c78ff1a8a6d89342806
SHA256:7a7e4dbaaebca073b2bb9bc3eeeba34ce5496be0a35b62bce19b461b43218911
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: it.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/it.js
MD5: 368a1232972a0c4f634c76db78e5b498
SHA1: dbb121749285ea1340cf147a3f44a3cac915e734
SHA256:7b9aac4916b04925b60c3ed0c3f65adc48373d479b6d030b216b4f031401e9f8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: ja.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ja.js
MD5: 64c8b443274c245de92530cf50ac8706

SHA1: f567bfcd4417b6aeae2fc38edf748924b1181efc
SHA256:53276c8771c3de2715c9ad8eb2826d997f0d8830ecf2e333388ff0c27d6ac30f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: kk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/kk.js
MD5: 3f9a7601fd781bb6c65059c58fe96989
SHA1: 189054aec78882a40f812d5cb9b300f452872a7f
SHA256:37325ef03f35faca200aca41e278c54b67e437ff81e74147480598470e43b2fc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: ko_KR.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ko_KR.js
MD5: 20ef64c247eff15d94fabc02896a15c6
SHA1: 4ffbdcdd647ae10e4b54b50a1722ea75b8a9e1ad
SHA256:85fe5b45bb8b659b296a16663f03987bf40ec88099d52a4d1d56879665d6da2b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: model.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/models/dom/model.js
MD5: 92ced545d85674979fcf041dd336c4c2
SHA1: 59c863fc616432ef9f8deb94775ed30f5efe7c53
SHA256:f6288507c20f27bf05fc71f1fd6195ba9250ed5824563d974073df7ec7f7a9b4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: model.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/models/dom/model.min.js
MD5: 0be9c51d1eeca6cf0fad0c30a1a9be6b
SHA1: 71c445919637005e5abb8583132208ff6a5a2e18
SHA256:c1bc9a11c9bd19e5aa7a538829a072bb1a24c6aae021c1607a49e7dcd9116aac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: ms.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ms.js
MD5: f0f057fe6321dee6122f9dc1a0aebfeb
SHA1: fbcacc7aac260a30a4c6213687aa7f3371995c83
SHA256:abff2edcfb4baec1ebd93c681f58fe893a09d56a3a6c9ebe8bd51348dd78925b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: nb_NO.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/nb_NO.js
MD5: 776be941e0917d4513e0beb2f8e18e99
SHA1: 164b9c95814d8941940485a56e8d5c2144fd2693
SHA256:4e2aa817da52cd69366fdf338b40d6e4284f521156b9e73653b468327431e3df
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: nl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/nl.js
MD5: 5199e61a9d49f51233fa4996003bc1bd
SHA1: 19056a6dd9e7a5ca3f77eb810d821fa14c6b8ba9
SHA256:5620e476f2a53f177ebd3dce0e5e1d0712922784e25f4a4a7e4ebd61133dacfe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/package.json
MD5: 9b9b3b959569ad4047094f7f57c6d0b0
SHA1: dff4699f85147fc84e9581cef8e5cca6d4ac2898
SHA256:1812f660a324b0bea0b9241e49e30bbc191babdfaf19e1754afd4b8975f308c4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: pl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/pl.js
MD5: ad4d61e73b6f7c576bb2d042b7c6ee83

SHA1: d88f3d98055cf7ed05a82402fe97fc5e08c9a2e1
SHA256:9d0dfe442f6fe41f504a97ba8154fcc35d4cfd011c518f5812bf8afc5d2b4552
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/accordion/plugin.js
MD5: 0c26a8f224595cfdfdfc9e3207153998
SHA1: e73d1e35b8756c82d89dfada0c949c514e72e5df
SHA256:59dd77687b20ad3300fa6f82b67eca40082abfe0bb4573bb912ca5df3244752b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/advlist/plugin.js
MD5: 4cf798ca742822a0955b61200999c86d
SHA1: 08861f1163a7a05389cc551f288fdb7ddd85acda
SHA256:0c5619a06f7fd37458e63d6f4e3e40f671922d41f42568c12b35337c62c6c716
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/anchor/plugin.js
MD5: 00f03d1628d1607abeff03dd48069a07
SHA1: 61fe61dfadbebfe5704a5104d3be47255fa0bf4a
SHA256:f1d323a8a66a27b3d1268ff96669a6396d13f5760f6fed28c509d6afd87f8e3b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autolink/plugin.js
MD5: 3c2b9d9af1f2066c8fab92ac6e3670fc
SHA1: 65f316de2c7b0af90b2da856eca594f7dee06f8f
SHA256:82784fdc1ab46744578a785a3a760c91bf8a48688fe72db53dbe452f2e40c3ca
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autoresize/plugin.js
MD5: 743a57e49b518031967986ded1def389
SHA1: 80fccd10cd82fb623fb8d7295fe893090a8c58fd
SHA256:8b23967af0cce0a26c29dd0bd7acb4382f83ceebab3c56dc021fcbf350e5a1ac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autosave/plugin.js
MD5: 3ee2a6b074950f82461baaacbe21b93b
SHA1: 3c5e93053e300c794576523193b1f24aa99d8019
SHA256:3ae5d7d31e44b20c1ec8d139d6733978ef8383444853da806d2d8100c5fe2e2e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/charmap/plugin.js
MD5: 9ac976a3bf68b6b6c091005f73d04fab
SHA1: b0d353f8b4541a7cc178eaaf2a80549e7e8ff2c1
SHA256:1a668ce204f20430c3ef538e51e3862151eedf1bb3cf101b1afbe7cb708aec9e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/code/plugin.js
MD5: 86b743c2c6ea9edba2ec738138af4f13
SHA1: 93681977da421bc8ea3d1b9bbb76de387b1e8a8c
SHA256:ce338279e8d050f97cc7becc25f107df74b83fdefe4ececf04c71b0d416f5358
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/codesample/plugin.js
MD5: b2f0960f34d600ad25d1c3ca586716e1

SHA1: 2c12a19e0992524387d66dcba06de100f2dbf154
SHA256:ba8be2ed436b2d3381aff465c2ba821144b78322a3bff19a2c65020149d3a17b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/directionality/plugin.js
MD5: 3dd9a890f564cb1d56ae8b6e3b1c6b0b
SHA1: 74aec8f641dc279d5f8f8a2b665ba85ebc1aed34
SHA256:e9418500feaa7df5e03cdc0d2ae92fbba76c952c7bbce37d3e265a1fffec6d09
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/plugin.js
MD5: cf01297c5bd4649c96d4b02d101dae91
SHA1: 21c76ac83f3097450701e78cd5ffd33b11f43b4f
SHA256:34061d4ede665e92dedb70509872a51f60568da62c8e25196bbf6542b56c1c5e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/fullscreen/plugin.js
MD5: 28c739ae4a156c2b70425e67894e0cfb
SHA1: 9ace37e56dcc3a1eb548e0433b6b6cdde8bdc973
SHA256:4644b705f6a4c2100f872f609c182b4e0900b090db72703d6e1c48039a823e9e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/plugin.js
MD5: 253f38446fd2cf7dfbbe9b880b61e880
SHA1: e9bfe599b7f091c02bd0ff8c46a6856f4abf09d5
SHA256:dce11133546c5085b70af66e13f2e8aee2adafd450a82d60439bef5c0728632c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/image/plugin.js
MD5: b974ef4261f90c66ae8a68c401aa0916
SHA1: be2d43790c4009bd4c72d82be5ad066e6d8bee3a
SHA256:d9b1c6f4e74f6f4240635c755dbfc94f6316d574dd8eb45c48b537cb726bdd22
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/importcss/plugin.js
MD5: fe5bd836613008ba3e14da66426e6cf0
SHA1: 53f919fb96bbe097912091801edcaeaf57f63360
SHA256:2c28d93c602ed624b70acaaea8065f0b0092385c266f0c3c0623a81d9d31a137
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/insertdatetime/plugin.js
MD5: d464db74437fb538b365409be1219fb8
SHA1: d606acca83395c58ef32b16e836c51d53917234a
SHA256:1e2f8a916c73de235b738f5e07542e95e2431792a85c2ac3e0a5c2d391b5cbe1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/link/plugin.js
MD5: 70f276d56ea4c8640a375ea6774b2923
SHA1: 76e084257759299ad236e421d2fe7d8d1a9a372e
SHA256:e1e073821da7551dc30ddf211e891d6dfc3df64b379d0249dc1cd2b9c0368dd6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/lists/plugin.js
MD5: 138ba109b4063f503cbb7e1064cfc881

SHA1: 2ca024a0c7b7336bd76402c5363091a420c15ac3
SHA256:396e497050bc5187816eb1fdef252265202a3ff014f4556ede18f26fcf50a1db
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/media/plugin.js
MD5: 8389bb07d879f4998b51bb536f098c45
SHA1: 5e70a5ff66ef5c44dd9da08ce45cd8c64d6e8a66
SHA256:ef9bdde625746627bc89aa1e805224e34e13b1a67a6c8ab93ac5623bb01c04ba
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/nonbreaking/plugin.js
MD5: 4231e982092fc8f5dcc2777c40382df2
SHA1: 421b576c14bac6172fd57f8411e34925c46b990d
SHA256:99e622636595ccd5f40a10b1d5745520c5aab64eaac95158a0794dd47ddc74b1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/pagebreak/plugin.js
MD5: d67bdbfcfc78a4cb39351f3fb655c92d
SHA1: 637cf76c18f406bf636337a19629394b37108fe6
SHA256:3a8fe47da93bc621dc3d68599ecfb5280b187785d557afc5453db7f1fa7fcceb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/preview/plugin.js
MD5: 90337a569238aa91fa0792a508445f3e
SHA1: 4d36003f7d0d96702f72215e2cbe351492c85439
SHA256:b7c20d2574eb11039eada9c1fe7ee3ac2cba9d5f7b955602502755bb5e391b05
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/quickbars/plugin.js
MD5: 8d8d553c91a139fc4c224234e6970ea7
SHA1: 680f7e9636582cc56dcb4223ff0e59784c5b01d1
SHA256:ce08ab45d1c7e8a1e6d6bd58d544f41e18b5297110916f3374fba173f45a6ce3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/save/plugin.js
MD5: f2dd66230798978f2f2ad89bf1b47a44
SHA1: 4b423e6306670c0ccd68417ec27a967837162524
SHA256:c7b51ba5c175c0199ceb2c3e99ed538c8bf38d27d6a184f133269841ff1b4df0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/searchreplace/plugin.js
MD5: 08c76bf5f41013c910a4d7e6d7f48625
SHA1: 5b1600a24979383659aed52adc6a51db2dabf04c
SHA256:2929bc87df688269b9f7a35e4d4a29552907034943381742024 9fef09861ddb2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/table/plugin.js
MD5: 44be7671104c6f32a8dcd8f959a9b225
SHA1: e870f66c7c730d6b8464c9321009cbdbfeda856a
SHA256:742a8d2e64b72875ec62c26eb83a0e6864cb042449ae1ea30862e2f5af9d6727
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/template/plugin.js
MD5: 3a4c4955d1b4d889c3d416606ebb9f83

SHA1: 27e0e2a96bb44f7e14115fbba49c43671fc168d7
SHA256:8f13acad6f65b050f231f21505490f310f199b7107db5b727cb82051dec71c84
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/visualblocks/plugin.js
MD5: ce6d5eb4e92f4337a3fb5698c38e095c
SHA1: 25e545c6568c2cf49f5dbcb868fb2d8f14c7cfc7
SHA256:5fafb04cb5ea7a8b450eaf14376f01d361c72c73f8e85edc64d67ea3f091aaeb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/visualchars/plugin.js
MD5: 96030048a7b8426af8e7d86ed3b7dbad
SHA1: 6ce30d628d5a3a07b8caef14834c7f6e6be55aa1
SHA256:cc521685cfeb0fdc3df6df7cc7b65300ca862d80e9d9f6ab5beeb39beb016032
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/wordcount/plugin.js
MD5: c5ba19d0d4b02655f0ed55415e932137
SHA1: 12673e738273cead65023dc694e13e3830f24780
SHA256:f6b2997cd7a8b5c2c78e98cf3009a638c91f6b3865a72cc3a872794f62325b8e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/accordion/plugin.min.js
MD5: 067e603ad5c5f674309a354ac1b417a8
SHA1: 2c5627a27fd532239d405a4ee988b9aa8fdb546d
SHA256:71e01f4a32b81fbbee5839f6d7cec3c494a1255fcdf109a4b33f351a92da3dec
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/advlist/plugin.min.js
MD5: b319374c0fb1c7abb405d2e8fca8302e
SHA1: dee9013b4bc799abc83498122289386a09dae954
SHA256:1a93b817161911b851a32ce480bdba8dd0011d795bf4936cc551c307c924400f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/anchor/plugin.min.js
MD5: b384c952c6cd6f98bdc3c4d76d5bb897
SHA1: 0f519fcd4787dd83d9bb518fb77fe0d06d676b99
SHA256:b346122f0718a274c470af66739a576e20987f0f40c2681fe5c4c71a73c9d805
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autolink/plugin.min.js
MD5: ce03bbeea10d77366f6cbeeed1e83629
SHA1: 0a035fc115ef5e33197ed0c6e2ba7483a1c6859e
SHA256:a44c94ff03577d9501e970cad55ec03e1521e36ef1fccb84dc44465e7abd5d1c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autoresize/plugin.min.js
MD5: b1d111c57af113260bbe0c9683f10f81
SHA1: 64d3e6a624c7667ef0583aee80d7e33359ced120
SHA256:03899363894652e3d0ab174bc7b3e7b9a15233a9c393b10a8b99dfd19f948ce0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/autosave/plugin.min.js
MD5: 9919c6500988b48e5dce210fa5a22134

SHA1: 4e6c5efa279b727356341654118f8a86c24664c4
SHA256:3033e8dd40ca1d6fca456cad2b7c13c8fa09941373f475d624576a45fc9ec38d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/charmap/plugin.min.js
MD5: d8ab4a580f4942d6d8f1d6ff516db282
SHA1: 716aa67c593f9fd259d19ac733432999aa2d3ad2
SHA256:aef9b781c34c04c4489888b7e11d5327a33e85f9e1d242ad39b81ee88cd9aef4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/code/plugin.min.js
MD5: 9bd0ef3497c2d1e2be98e6c9f5c8d523
SHA1: 00bec4bae4d8d8522663f2f223c9f4d09823a7c8
SHA256:3a0ffe7657ba037e5698e88ab8f71166a26f356305028fcdd30d7fdb71fc6d70
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/codesample/plugin.min.js
MD5: dc3bc94210f7073c847f80667595d448
SHA1: 33443c4a5e7ed6e53607cb12089f917cd83f6bd9
SHA256:20fad89a98983589acba8a9def528fab457b6c9eaf47dfa1793d9798c14fc2f1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/directionality/plugin.min.js
MD5: dd93c2710db307b10e17c75753b2ef07
SHA1: 6cec303fdb36d2ce250b63c5e838b6bda3e12073
SHA256:679ac922d968578dd0f77bdc530adb6601b85881c5411190c4bbcd2db7cdf38d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/emoticons/plugin.min.js
MD5: 47b6c0551c44b85bbb8ecc921861484d
SHA1: cafb1171088286600c8a4fd0643195b86f0f9c0a
SHA256:d3ccbc8bb44bad7ec31776be275e6c695e561a1ccd86d7726209d22da8d02160
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/fullscreen/plugin.min.js
MD5: 2e44c4577484dbcc81804262f981dcc9
SHA1: 9070a3b0b1f5a5f84a4b61a2ef929a679aa9aa8c
SHA256:36c09c8ba092072367eac8f345b17c99b061f2b3ce863bd0a6dcd12135afcbe8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/plugin.min.js
MD5: 8efb996c1bb1575c22a07e252c92dc32
SHA1: 82064429652916a86f9138eb306c5bf5b359b4da
SHA256:9a4183d5155768e3eda6f91d635b4faab5a435b008930b7d64366262d47fb63e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/image/plugin.min.js
MD5: 4ee4e878aa3adc242c538a89f232d438
SHA1: 4c8f4b5ae6056141c3f635c20e93f538f11074a4
SHA256:f4ae803e63eff67e37785df908d272b4eb8af889c0ddbcfa792f4ddade55b9c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/importcss/plugin.min.js
MD5: 2770b3a50c49f2369e17f6d0459a8e5c

SHA1: 495e54d14da9e72783564e52128bc92ca1c672d6
SHA256:19ed5f9afe0e409d3f9c09c2221d54f5eb0f6d381ab47dc5380ea2002e5f4e30
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/insertdatetime/plugin.min.js
MD5: 8aa135fb5a99ff26f09571d53cb3d71e
SHA1: 3f9cc4a074f911e341a07449c882717d2accb283
SHA256:45ae0ec27b8c94461e553a2ac51c7cccf2c5137337092f44685d08df64b6ce21
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/link/plugin.min.js
MD5: 8e89716493e1c3bd9ee64cf7011dbc8f
SHA1: 993553840acc116949afc32f0e0ea0c38690d697
SHA256:c3380c68c1309942ea2c771c7de8a79229420027483d94c5b435e0894253b4de
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/lists/plugin.min.js
MD5: 7cbc4e1798bb427bbdfc3900ed86f480
SHA1: 121fa46d2e7c32ad7cf8840d0e901c508c57171e
SHA256:55ae482f1710f31055ce7b0705f49879813cf688428c8879c7e8d08a2ed32e3e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/media/plugin.min.js
MD5: 73c818ec06d11d2b993d2618e0a8bd57
SHA1: 99cea7d880d142cbcfd76090e71417a78f4dc447
SHA256:35be1e038e28c8a51c3d514619713430c42954bd9a8762beafe28cd3409c60ba
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/nonbreaking/plugin.min.js
MD5: 4efd4e53a2805970767659d446a1f4ba
SHA1: 5b68775c61ddd35c9acf041d16f67ffb66f10332
SHA256:ac804bdf080ab46ea92a9b68c90bdb0e99928164c74af72b48b11378a23a58bb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/pagebreak/plugin.min.js
MD5: 7b414356e50f26d00e799d5408c5e352
SHA1: 0799616465d1bd686a386300896bc2d0a92e8a8d
SHA256:199a685f1357aa31673f48f0ad35a5b5d071b968264e6690c626e2fb211188d6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/preview/plugin.min.js
MD5: 7b4fda9f4cbaf1efd561bffd8d8b5dd7
SHA1: eb3cfece0c9f6138814e88bcdfb14f4e68de2eb6
SHA256:cc655800f2d98cf0d394b0f9c3e1f3f0b8c69c27b27220e6770c875a6a71ae7f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/quickbars/plugin.min.js
MD5: ef8d3102fcd9b08f277d4cc6763a3be1
SHA1: b513a9b10027ed24161fc2b09d7e239dfd2cd676
SHA256:c426447958fa155cfed43956a043afa2d948612879d19db4106c228608e371c7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/save/plugin.min.js
MD5: 176275d910430106123f823ebbb6cc9b

SHA1: 787852864f220b7c65c25cd9b8600adbf83a202e
SHA256:d103599c347262a78ea4d1201047ecdfc7862a2ca70d5292f6725f1c2c93d061
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/searchreplace/plugin.min.js
MD5: 92702585363ad2e0f4e1e248e6f9a9a8
SHA1: f3ce94cdf2f4528cd10361ca4da720fa43868200
SHA256:c428e2ad41e4e5e996a6442235a9751465deafe1d3f79d8991a90ef0a01d9484
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/table/plugin.min.js
MD5: 6eecb7ab130b79964f3be2fa0c31acaf
SHA1: 42fa499b5d0a2e918953ba561c67f5c2d9453760
SHA256:dc1ca999ea704e4c0859be26fa2bb7a72eb70e8a354b9e2c6e0142fac609777c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/template/plugin.min.js
MD5: 9211d3b09727101886e577af595a5a90
SHA1: 42b62808dda698334e7c1ffdb9f4a2e7960a02f7
SHA256:ea6da334ddd8e383edeb782bcf24f7934219d56ebe7d307021de71b38c34abd7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/visualblocks/plugin.min.js
MD5: c272677f503df90e9eea5184954a1fcd
SHA1: fee72d8fc391afca9b2fa5484286bdd09d875fe3
SHA256:4d763671681ed728cdafc3d3feea7859b2105c2cfc572c75e8b21cacc0def500
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/visualchars/plugin.min.js
MD5: f9a9ac81c12c2d716964e6b9c6c264d6
SHA1: b21396cdb4bf5bd3c8ffae9f2c4900315eadb2a6
SHA256:66f2a410f017c9932b227e7ce10bf53071f069edb904b11fb24a2c5b783b1969
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: plugin.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/wordcount/plugin.min.js
MD5: e1bc9c27e8c05aba5da89485ea29852b
SHA1: e223913921f10e9111b3a154130a25258acf76c2
SHA256:d7ba7e574630df5367fa5ce97a9d5d048f375ce026333055639039046c7ee239
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: pt_BR.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/pt_BR.js
MD5: ca7a4eeff4a8529a84f3ff5e7f1fbd4d
SHA1: 301b5e181620e9a86b8e0521cc3f56835f98a0e9
SHA256:571938497a73a22fdc5ad20de30a0d6051b489ac787659a73dd6927f73bf813f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: pt_PT.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/pt_PT.js
MD5: 98c786e104869984b866baa8ed1cc414
SHA1: 70386a8fcd314249ce73542a259404019f40fe56
SHA256:f9fcbf81468c7312fd52504380f411df09c2f59cb2a1647c6d0cab5f3f414b9c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: ro.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ro.js
MD5: 954a4ab723e0f927235bcd3020c8e0e7

SHA1: eeb3638b56c77058c31193b95ae72b4811ca2e92
SHA256:1e0e4e94519949b7e750007e7193e3d3a20855f57b5ff982a985edb0718f885d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: ru.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/ru.js
MD5: 1d302511d2a9b1a0a765358559e6ed8c
SHA1: dc2960bf5917645f7f007fdc082efedce924e695
SHA256:019be56e2cd8f3a4b7bc028535cabaf69c075744666652bcd40edd8483d543a6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: sk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/sk.js
MD5: fe4a80d8945887d8dcf20af8a3c1352e
SHA1: 36a21dd701f08b0d0acfb8294f006762fc424dde
SHA256:b259ee9a894fa2cc41a7900fa637a2aa8e4224be1f4ef842b541f977240f903f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5-dark/skin.js
MD5: 33bfe3e522c9bcc81a0ac4a754d0fa01
SHA1: 822a6e8c4751f9dda822f84703ee522f7ce0ccc1
SHA256:bbf5986c65426afbf26be7c0e5de03fa8e68d8f2219e2919001f1a10b173a952
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5/skin.js
MD5: e955f1a8b28d4fc0e3ff9437a54cf3f0
SHA1: 7523ca2c72f80f957cce1cff4c6f697266e0b425
SHA256:963a34799e5790f24ddf1824583cd10f3ba9c39db04e5ec60a5cf11ece7fca31
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide-dark/skin.js
MD5: f1e6180bbc9af02f6eadd4fb72053f8c
SHA1: 58a5ea6b0767562cf4db3aa7b4f4e8bb1cc53dcf
SHA256:5048d4c092234ee6ca7dc7cc764f9539b3dd8579355f4b64a30eaff4d05bf654
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide/skin.js
MD5: eb819709d0ce9c502c5b7ad421407d60
SHA1: 9f75d43603bdcd46cc03bdfb67071160409dc91b
SHA256:5a3d4132dbd49631dff83665fdc93242175673ee02a44c25303038edd70b7037
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.shadowdom.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5-dark/skin.shadowdom.js
MD5: d738bf552b3156b0a77176ee6602cca5
SHA1: 268465839d61adf3a0b0672f8ffdecedfaafb053
SHA256:d24a492050fb69964cdb38329571b9fddd1b0834d3e7dbdb408dddd58493ca2e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.shadowdom.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/hugerte-5/skin.shadowdom.js
MD5: 20b5197219c55275d0b70c53fba64ed4
SHA1: 1e2c40c61236d680b9a79abc119fe7e9a0134f81
SHA256:afb05e588c7480e5fe4659e23d1455fcf4d50d88ceee199989022fe3af1fba44
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.shadowdom.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide-dark/skin.shadowdom.js
MD5: 1e892ba61cc3e6d5bfec63dc9cec18c3

SHA1: 84dbd80ba099e183e44debb25fd01890797707cc
SHA256:60f0ac19cbb0903f7fd4bc8a1fadb16e818d45b1908db27a89679aadf6fd6332
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: skin.shadowdom.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/skins/ui/oxide/skin.shadowdom.js
MD5: 731f24060ee9a8c936071b8765cdde89
SHA1: 21f37b358ef16cc9fab3344261a2236b0260ac0d
SHA256:bea22e87cbf4ff22524e43516d28e285d0f096409d7891fb6e91aae8fdf56eda
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: sl_SI.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/sl_SI.js
MD5: ac35121257bf831e811f75c28c471dcb
SHA1: 5e2e75c81c74714798f3ab92f1cbf4889a705830
SHA256:f001ce48bbaaa6e711eda1b603d13edc38f0c2db5592f0f8cb3b798f001b6e17
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: sv_SE.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/sv_SE.js
MD5: b24075bd395a8abe5e100788bba0a74a
SHA1: 699908a684581883ca84b7f43db273ee83d68245
SHA256:24e435fe459e6a809eb78b0b66c0146226482f29cf4caf7c84d6a09889a5ae25
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: th_TH.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/th_TH.js
MD5: 0f0c790204d30c81b6645735545d20ec
SHA1: 5fee086306a6157bfa9758380c9da89040dcfaa4
SHA256:38e2e42abab10f72d5ea1f17714112c287f350fcbca05c5906ced9d3595c16aa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: theme.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/theme.js
MD5: cf817d8941a3c0111193ece2d7c9b929
SHA1: f7a71244e44dcbf90a9804051bd788b293289a8e
SHA256:8e0f595de763e6ede53566f5516c6744a175fabd46c40ba3cba6ed39140bb926
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Identifiers

- pkg:javascript/DOMPurify@3.4.11 (*Confidence*:Highest)

remotegui.zip: hugerte.jar: theme.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/theme.min.js
MD5: 8bf8c393660a3656dc0e4b9f12bdc697
SHA1: 49a25ecc5db9c1e0f63804f3ab89885d7d0119f9
SHA256:a43e3e8ec4abb5adff7d91c3c7fe12323920c7bccbcd47ba84625353a012d513
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Identifiers

- pkg:javascript/DOMPurify@3.4.11 (*Confidence*:Highest)

remotegui.zip: hugerte.jar: tr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/tr.js
MD5: 4543135c90640b64ea11bd4ca58192b3
SHA1: 93c8cbd63e67d56b8943946634ebc319efcc8302
SHA256:fa1b123a9dc42af696b525c76386e38f2abaab07b29d29fca957a3d82feb9170
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: uk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/uk.js
MD5: 64c0553a6c8b19667964e263a03dab26
SHA1: 998a732ac0b403137b79178d83163accdbbcad27
SHA256:0d63c3d3ef18445fa032a6b4f8d6c80c26bebc6eacb71dc934d7b5666453b2a5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: vi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/vi.js
MD5: 85d7f56b3ae07bedcadde6e04251dc9a
SHA1: 5333ccaa75ac528e70e6d3a50bc47a46573dd353
SHA256:a8fd67b418a1d1225ded5342c6cb7ab53606818c22b7a964148c74cebfabd0ff
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: zh_CN.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/plugins/help/js/i18n/keynav/zh_CN.js
MD5: 93f3f1526fb8af6be6fea9c9d4cac78e
SHA1: dbd189b2ee499e1be666408ccd83b41c7ee84bb5
SHA256:5f3a261a4604bf1e7116dbdb1602f87bb93e324849b64227398c8b93113a38ac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: hugerte.jar: zh_TW.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars

/hugerte/1.0.12/plugins/help/js/i18n/keynav/zh_TW.js
MD5: e3325e4ccd2fbabf42e18053b168428f
SHA1: 6c105cd27982cba07413ba280b946ea010c9ea5f
SHA256:5f8f7d1e97005d84e3f868727db6c36baf3096f1cd4d14effb7ecd33ae0ccb1b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: jquery-ui.jar

Description:

WebJar for jQuery UI

License:

MIT License: https://github.com/jquery/jquery-ui/blob/main/LICENSE.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery-ui.jar
MD5: b8e23816d55710b0e639ee4f09fa6f69
SHA1: 0139174a3781a5d7ce14207f5ad2dfb32d4647ed
SHA256:baa9723c6162686404dfeea20d613e5f7da678828a41f74b8bf3c6df50997589
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jquery-ui	High
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	org.webjars.jquery-ui	Medium
Vendor	pom	artifactid	jquery-ui	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars	Highest
Vendor	pom	name	jQuery UI	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	jquery-ui	High

Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	jQuery UI	Medium
Product	Manifest	bundle-symbolicname	org.webjars.jquery-ui	Medium
Product	pom	artifactid	jquery-ui	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars	Highest
Product	pom	name	jQuery UI	High
Product	pom	url	https://www.webjars.org	Medium
Version	Manifest	Bundle-Version	1.14.2+1	High
Version	pom	version	1.14.2+1	Highest

Identifiers

- pkg:maven/org.webjars/jquery-ui@1.14.2%2B1 (*Confidence*:High)

remotegui.zip: jquery-ui.jar: jquery-ui.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery-ui.jar/META-INF/resources/webjars/jquery-ui/1.14.2/jquery-ui.js
MD5: c0de2a664d670963826daffef7b9bc08
SHA1: 346bf6792d7bcb979a04d86922e59504a107a760
SHA256:5a171a6f49bb396484b96d8dfa4a557f179ec1d9f0d7a34090bb767f0e7e8d1e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: jquery-ui.jar: jquery-ui.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery-ui.jar/META-INF/resources/webjars

/jquery-ui/1.14.2/jquery-ui.min.js
MD5: 6df56c01471a6c5de0ca276ac17ae002
SHA1: a84e47ebe2b89723bdddd9958ec52f5e88111633
SHA256:d8e85cec7f90c5bcc6bee2db08cea9acd6a10229d84dfa44af19192704b644b5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: jquery-ui.jar: jquery.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery-ui.jar/META-INF/resources/webjars/jquery-ui/1.14.2/external/jquery/jquery.js
MD5: 12e87d2f3a4c8b347ab13a0764d420a3
SHA1: 4be715e11048c057fdf2ee0fbbfad4dbf3504c55
SHA256:78a85aca2f0b110c29e0d2b137e09f0a1fb7a8e554b499f740d6744dc8962cfe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: jquery-ui.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery-ui.jar/META-INF/resources/webjars/jquery-ui/1.14.2/package.json
MD5: 9639325c0c96e9184672e756c05513f7
SHA1: fbd0a319dbfb1198e319ae964554d9d4cbb85a68
SHA256:3e6af46e94a453cd95cad6e04b434699614cc4842eddfea4fc4e739421098763
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: jquery.jar

Description:

WebJar for jQuery

License:

MIT License: https://github.com/jquery/jquery/blob/master/MIT-LICENSE.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery.jar
MD5: 4af65e569248d8a2411f66498d720280
SHA1: c3dc40b1b5f24c56afa36fd9a463bb9f378ac4ab
SHA256:de28c4da0ea9f16101352dd3582ec8021ee5e2de5f45104ca171876003d54db6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jquery	High
Vendor	pom	artifactid	jquery	Low
Vendor	pom	developer email	james@jamesward.org	Low
Vendor	pom	developer id	jamesward	Medium
Vendor	pom	developer name	James Ward	Medium
Vendor	pom	groupid	org.webjars	Highest
Vendor	pom	name	jquery	High
Vendor	pom	url	http://webjars.org	Highest
Product	file	name	jquery	High
Product	pom	artifactid	jquery	Highest
Product	pom	developer email	james@jamesward.org	Low
Product	pom	developer id	jamesward	Low
Product	pom	developer name	James Ward	Low
Product	pom	groupid	org.webjars	Highest

Product	pom	name	jquery	High
Product	pom	url	http://webjars.org	Medium
Version	pom	version	2.2.4	Highest

Identifiers

- pkg:javascript/jquery@2.2.4 (*Confidence*:Highest)
- pkg:maven/org.webjars/jquery@2.2.4 (*Confidence*:High)

remotegui.zip: jquery.jar: webjars-requirejs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/jquery.jar/META-INF/resources/webjars/jquery/2.2.4/webjars-requirejs.js
MD5: 30e1a7f167b667001f50e32ea87bf7b5
SHA1: d18dc733350ad3549af2df096599e824c10f777e
SHA256:daca7b23bc4d8302a8961373b92b78d36d5c85d730fc14130e29d55d976aa420
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar

Description:

WebJar for moment-timezone

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar
MD5: 9e4e844fda6a9b3c6964ab1051c7855d
SHA1: 8cf36bc0f20de5921597e2c9624c852ef91bd5ce
SHA256:adb08a2d8021b21757d6cbd999278ba5d80f881cfae845ee5aeeab93265aa3b2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	moment-timezone	High
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	org.webjars.npm.moment-timezone	Medium
Vendor	pom	artifactid	moment-timezone	Low
Vendor	pom	developer id	webjars	Medium
Vendor	pom	groupid	org.webjars.npm	Highest
Vendor	pom	name	moment-timezone	High
Vendor	pom	url	https://www.webjars.org	Highest
Product	file	name	moment-timezone	High
Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	moment-timezone	Medium
Product	Manifest	bundle-symbolicname	org.webjars.npm.moment-timezone	Medium
Product	pom	artifactid	moment-timezone	Highest
Product	pom	developer id	webjars	Low
Product	pom	groupid	org.webjars.npm	Highest
Product	pom	name	moment-timezone	High
Product	pom	url	https://www.webjars.org	Medium
Version	Manifest	Bundle-Version	0.6.2	High
Version	pom	version	0.6.2	Highest

Identifiers

- pkg:maven/org.webjars.npm/moment-timezone@0.6.2 (*Confidence*:High)

remotegui.zip: moment-timezone.jar: index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/index.js
MD5: 16b10b9be0471f35921bc17b645c6fcd
SHA1: 7e9c41f04cff37b876169e1e5108b5b757305822
SHA256:b93bc1a0ab15d56e12f0e281bf005d39166952d9208b828e8d056563f3ff1fd1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-utils.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/moment-timezone-utils.js
MD5: 75bc3e8ef0f86917da40a0c439a4eed8
SHA1: a7ae8afbb2f4e81f7ac340c61ba0dbc569915506
SHA256:0540a9793f93353fcf87953b58190fa57737d0b7004259b2aa3ca587dd330fbb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data-10-year-range.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data-10-year-range.js
MD5: c36c98003ca8dcb66a3555966ca4620d
SHA1: f1a3bd439e65152780687ea53e958ab46151fb39
SHA256:dc5838239aa616be1c3bbf6fcbf6627b0db08ab42204817094ccfd4ae5aed8cf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data-10-year-range.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data-10-year-range.min.js
MD5: e75a635efb17566ab9720a5206ee470a
SHA1: 0a567e0241d5d695c31d9f724e286384931aad84
SHA256:9c1b27e166c9e015ddc067455a146fc7bc3f68c4b3d1088198cc0234b4669773
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data-1970-2030.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data-1970-2030.js
MD5: 43654ee70c266b87432d63d4b7fe58b1
SHA1: 17c123f5d9a7fde79b9f99b570599b37810673b9
SHA256:903064d5541c5fdc7e6b2d1b26dae4053b6650b7b227aed8c526a97ad91eb254
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data-1970-2030.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data-1970-2030.min.js
MD5: 2d8331f592180f4d4086463dc7c9c819
SHA1: 9a1c299aadde4ca774ba8c71b754a4e9b3f9a247
SHA256:a70de767c4733b804dc38ddd9daf67d5769aaf8b1cbb4667582dd2a1fe05f8d2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data-2012-2022.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data-2012-2022.js
MD5: 68561b0310707071f82747e5f36e3bb1
SHA1: 90183f32430b4d323119176bdc1d53067c44d601
SHA256:8a5c4585e2743e9f281be8f61cd41e2a3a6b7295145c6ca028b228e5ea531d15
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data-2012-2022.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data-2012-2022.min.js
MD5: f55192a7aaf0650f87fa367d216fc5c3
SHA1: b126c2e1c8c11a545c0103a01ac138a3c2c1c4e4
SHA256:08de8c53033bab3a1d6b48387f4bd5e1834887f1d210441eb848cec8acce706e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data.js
MD5: a50e636b759ab7da8296808759977a6e
SHA1: 9936a764c9f61284e82f65b07b39de6e2d1bad7d
SHA256:abc3ab7764bdbbda34a3b62594e4ca02d96b2ddf3e9924830a76c7a5d630179d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone-with-data.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone-with-data.min.js
MD5: 157431c1e56a359bb2790ad47f2ec5f4
SHA1: 2dcef3b3678358207aa587931657b6f267fc4f17
SHA256:d284077858440902633116 7b88d91cc1fad9930cad5cb132fd45011eca4dc633
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/moment-timezone.js
MD5: c08d9adeabb5ed9cb664a6359f071e2c
SHA1: ddef54e6d823a167f25f0146018ecbf8ea767422
SHA256:80c8539b66b9482c970a6bf4938b25c9e499e3aff6c37da7ed64b9f44e1d47f4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: moment-timezone.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/builds/moment-timezone.min.js
MD5: b008a08af336ea6e74472827ff10a627
SHA1: 5f29a450998155109f195d927c1609f3eca49f4b
SHA256:10bd0a9059948864d4b4e93ca9bcbf69b38c2ad9993b08f3c37f1a09d2263780
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: moment-timezone.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/moment-timezone.jar/META-INF/resources/webjars/moment-timezone/0.6.2/package.json
MD5: bd79fd3fcd91fb3fd4ee21c64ea3003e
SHA1: 6ec434b947651244ca1a0fe3a3c571aa5039584c
SHA256:bdb2ce97e3ad78759ad883cab67d3af9f2c4b36362b36ad6fe6ef2a574af99f3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar

Description:

WebJar for Moment.js

License:

MIT License: http://opensource.org/licenses/MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar
MD5: 72ad6b420b3b741d7def80f4837682f5
SHA1: 6087f9eb29294249887afa1eb4ec8308657c35f1
SHA256:71f0cbc7e4d2c943077dc758f7c8f0c7d48e1ddc7f9e7cfd27aecbc12712cfcd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	momentjs	High

Vendor	pom	artifactid	momentjs	Low
Vendor	pom	developer email	james@jamesward.org	Low
Vendor	pom	developer id	jamesward	Medium
Vendor	pom	developer name	James Ward	Medium
Vendor	pom	groupid	org.webjars	Highest
Vendor	pom	name	Moment.js	High
Vendor	pom	url	http://webjars.org	Highest
Product	file	name	momentjs	High
Product	pom	artifactid	momentjs	Highest
Product	pom	developer email	james@jamesward.org	Low
Product	pom	developer id	jamesward	Low
Product	pom	developer name	James Ward	Low
Product	pom	groupid	org.webjars	Highest
Product	pom	name	Moment.js	High
Product	pom	url	http://webjars.org	Medium
Version	pom	version	2.29.4	Highest

Identifiers

- pkg:maven/org.webjars/momentjs@2.29.4 (*Confidence*:High)

remotegui.zip: momentjs.jar: af.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/af.js
MD5: abbd3f78270e280c248535ca3e3b3e3b
SHA1: 489ddba9b2a2f15e2a8d59d751a45c5ed7041f14
SHA256:c59e2f2d09098829d00f5dab85e6ec623f6aa9e70285ec2aac12030a014e4161
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar-dz.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar-dz.js
MD5: 10e8f6da8f425e389f9dd462018dcece
SHA1: d638dc753916f10981ce562c7e7543944aa5755e
SHA256:2fcf1465ad9fcb33a1ee00188d0d8cb19e0d9094da9e27f56444b67e50c6810c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar-kw.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar-kw.js
MD5: 5ad9681e194f33543d33a588e2a21f09
SHA1: da190c4671145eb702d41ee980b985a9816bc9c5
SHA256:ebcd2afd129890e49aa91cbd6718916ceb743122a4d264c681a533d8066de673
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar-ly.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar-ly.js
MD5: 293c5c572f1e70336fb5a5cab29faded
SHA1: d969dc63c258a2c5587efa0cb2ac80034c44a5f3
SHA256:0a70bf3f66b074d68453af125059d60f1ce4d5a96d3401b0bb7f013fb7a56696
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar-ma.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar-ma.js
MD5: 6f5179b883bce68003df4d2c99caa156
SHA1: 3af849ad551cc126ea26fe472770b0f2c86363b2
SHA256:ae28a7c4d994a1d4059f2dc1e6385182f3d5aab262d637a6bdfc80f3e3f5471e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar-sa.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar-sa.js
MD5: 92455d26a00821fe9aba7ea8e23ec89c
SHA1: 18d22d6e22b460fb0d248426001e4cbfd9a69393
SHA256:4913900a380ed33b662fc5299fda05cfba74367870ba23f3d9db5dfd0775c876
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar-tn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar-tn.js
MD5: bf6b33329fd589f8b3b393f6e64717d4
SHA1: adf2dc833a46ad99f030b5761a7e6a97497ca764
SHA256:2b6a611f7d21a0752d9101347b22943dcdd91293f7e09ac11c3b04cee41f594f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ar.js
MD5: b0110c65e23d25860762820db7d2150e
SHA1: 249cc300a99b9cdc47ff3fd70c9b4cb22f0aed61
SHA256:73485f16cb9317f156bab05ba8a3233fa87513cf1cb52728fefc53703ffd5b3e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: az.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/az.js
MD5: ec1a4acd4aa555dd71722c2639df4db6
SHA1: 49b4198f1b008f9deeb9aa5d33e27647e812f0df
SHA256:21cfe14e920b3edc4bc394709929f61aa5f2f9e51d3ca0c6edd1e51f29d7e3c9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: be.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/be.js
MD5: 5c38f8d3d5da2b1b930f109553918781
SHA1: 181a1762773de78de3e2d21696e77a49a9e188a5
SHA256:aa0657f4f1e9f9ef3a3ce289bc882f5971195e4681499f02409486ed985e1407
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: bg.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/bg.js
MD5: ebd43c527dac81f273926142beec5553
SHA1: 46101d46348f560c622895e9e65465dd26e92d6a
SHA256:0d034309eedbd03f17e22dbd963c8cc8d490c8e877f39c6c4081636d1cd28fca
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: bm.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/bm.js
MD5: 2ef1c37399931e14e2a4471ebc57bd21
SHA1: 1e10777797f13333027873cf0a1e05e52c2a9264
SHA256:1f3217d69f6512ea3984fb7428e1afe0c7779cf3822582c52e6eaa8982ac23b1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: bn-bd.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars

/momentjs/2.29.4/locale/bn-bd.js
MD5: f2988fa9e29bc5573603a8140b321051
SHA1: ddca0b09ab220aa3e7d8b6d01e98b06071942e4a
SHA256:87296cd8b904b633d89b0a72b779aaf04e8d625fd8ed772e3227046b3a3acf80
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: bn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/bn.js
MD5: f5037a3495a3fefb37d9456b6745537a
SHA1: 5d8e28e5703371e674a9b2947426e23a1429455a
SHA256:a43f974ec15f638e67cec9d73cb33c339ce7cb35bb7041b478a930197977a890
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: bo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/bo.js
MD5: 7dc25ead6d51909386b03c060b891690
SHA1: 5b47f8a1cd1b1dad8e8ae1c6f408dadda7cd6983
SHA256:dbf83d196ab69149d5f056a2b44e06441626f1e5d3c3aa1a300e64dc5150565f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: br.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/br.js
MD5: 65949057a5632b430fce65f65c89ace7
SHA1: eda5bd14e942c85896b263b137e2e14f161836e6
SHA256:35b4113f7552400639dc76ea40d55f1be6f44af2eaf4289e7c37e4e657522ba4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: bs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/bs.js
MD5: fac80361cb7d5e0c44f8956063e8eb07
SHA1: e0f831af87ad28205b93fbe4d7ef9001227eb1e4
SHA256:1d185f2b71c18bb14d0e5db063d59912396d42a04aec97cfbbec19a5bb8bb5ec
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ca.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ca.js
MD5: 9c6c8738154552a40a29505cf41311af
SHA1: 65eee9703d130c7a90d085214ee60c4e087b9d1d
SHA256:c0ebe3bb033ce8f82c66a46dd297c19b30c80ba64036c721aca36a7f86f1b234
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: cs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/cs.js
MD5: 8f0a7bef088e6698b6a090a6f6fe22de
SHA1: b137a5adfe662d0b1c258fe7bb2b73b971e2268e
SHA256:0dcf511c06f565a917e4718cce467392bf898ba60af2b3fdb032b1910599ebc5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: cv.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/cv.js
MD5: baf681a1e97ac68186325a98d5ef1861
SHA1: c0433a02791bafe8efe6945a4ae0370c6d8d55b6
SHA256:231b3a65bc4beb4d6f0920962dafc82611403df4979655cea53d9740d2986904
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: cy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/cy.js
MD5: 868cca92c4392ae5b0627f305f9633b4
SHA1: 9c0f75132a2eaa3fdf0631a08f210f0e29208501
SHA256:05d100692e8cdd4a6b3b0eb56eb37c9c64dacab3254aaeba18c24689b18a6cf8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: da.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/da.js
MD5: 47fe4d0a5079542391abdcd125b4cb60

SHA1: 423a66383275eaf3f441f384c69b2d6e2cf905d1
SHA256:891e90544d1061ea578b51173a2dc4638c0e9af95cc2986f1f89ad5008e301e7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: de-at.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/de-at.js
MD5: c2df366205b041e50b0dc27fe427c54d
SHA1: c52be9218cfbe8ae8d51f78af3494d3a2ed5d35f
SHA256:0575c8ba66974f2eb3d7d74e16a265c40dbfe7802cefdecc9f196f92c0ecee97
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: de-ch.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/de-ch.js
MD5: 1f9bf40d5d392a14bb758de02e9d98df
SHA1: 838d95c91f39f7e28483c660e6f5005921d3da11
SHA256:b3c3d71abc98200d579cbbef89d470a6cbb272c4faa71e31232a68ef6451edd4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: de.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/de.js
MD5: 260cdaa4a123af8e02f5aa4001cceaac
SHA1: b928a076571a81fde7fc1fd4a2adb45d9a9a2279
SHA256:20fb0d0967e2720d135a6894165bf96e327b42bdedcbf45a9b2f9e44da7986dc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: dv.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/dv.js
MD5: b3ac7e877fac1116b8759c6e7384e86d
SHA1: 3321dfc6f7147d148167b23a3642212fb10b1b89
SHA256:94a1563faab9fe61f359a515042f56e2672886200e084de98bbd98769f71ba69
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: el.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/el.js
MD5: 7a1966e1fd7848aabcbefa28ff2a445e
SHA1: 29af743b2dd9c09d9962080c3a5b4cdac2b09409
SHA256:a73fa8b59dd099d28a7824980577379437273f6ef35a90409cf36492bc2b3600
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-au.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-au.js
MD5: fc0b9a852c77ef21ee6deb24d95769f8
SHA1: 829e7b64e421cc91fbb306243b31d71f06fabdc2
SHA256:6a84d80e99d57f1ca1faa1dcca9f48e9925de4013ac5ceab52cbf20b059cff8c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-ca.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-ca.js
MD5: b6f095c75787cb0eb2421b32b2e9ea14
SHA1: 415ffbaa1c99a53d233979f5e907e83b59d54c9a
SHA256:d7b47d71cd5b63a0cd7bc3945ca1799d9345ba9dc3e85356231dbb4f6becdd01
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-gb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-gb.js
MD5: 5ebfadfe47485b65c484822391d0aad1
SHA1: 4154fff794c0118f1c280d4e3c222b0b3f96a6eb
SHA256:46e86bfd873ce2ba61885faa9e0ba2ae1a510574f698d6a3aba7da49d1505eb9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-ie.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-ie.js
MD5: f5175b64f4c382500e7a00ed4113c3a3

SHA1: 12cf24c0dcfa4f82be14783a2889022043fe1f80
SHA256:41a3d03fb561db37dc1e3a63cba10467c0bcabb2ab7e788329f86b6be6f72d9e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-il.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-il.js
MD5: 8f131247f11cf746d1b477c75de2e0a2
SHA1: f1fbc068a029ca0fcb5755fc5211ae43c9b2dd00
SHA256:494c5f26d0a16c8c1645d70cfc327e19086831ce78bc98599f4e5abc321db7d7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-in.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-in.js
MD5: 2d5a9ac86d2a83833aec6a68bc8947ae
SHA1: 64d4492b47eac3212f09a9dd1fdfe2afc9721142
SHA256:290dd53cb6262cfc22c961faf969851adfa8c38b30c80c496b8c8f19232a13e8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-nz.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-nz.js
MD5: 3a68b41d7982ae7bbc8a396d23e9d1a1
SHA1: 0c30117c176ae1c60d35e54c3c0cd47b5104e28e
SHA256:9590cf61d2ab1b83f793be9f074340397e639fbb112a80c8bb7d2e3a77c45448
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: en-sg.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/en-sg.js
MD5: d32a209c24b07b617c68fb03e081061c
SHA1: 34729febed76ec17cccafdc06ce4f51902daaf42
SHA256:e3b29449d67e5d53d3420b5f4ec207dbd70f651380573b59f39aee2b1b9ca52d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: eo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/eo.js
MD5: f19d7f5dae34785b6ffd82971ff01712
SHA1: 8a6937235d4219a192ae127506cca9479097abdf
SHA256:823d3e21f85f9d3801f7004cc5cde82d5f45d98e977979322543a65908411e4c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: es-do.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/es-do.js
MD5: 3f09c253c2e7ed72706b062bdb3ecee6
SHA1: 3bcd2f7f697c4241a5f47985835b0190a643630a
SHA256:a1d29019dcff0ce2a11cdf97018c20e99fbcb739163c059ad8bf2408f77d3161
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: es-mx.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/es-mx.js
MD5: d16f10cddba51c3467b316318e592f22
SHA1: 4cc238005f4d59b4e3877449babf5cc8b3595f38
SHA256:a233573f641cc9c93c87b555fc5564c2e5ebb97e251338e971ba76e74d512646
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: es-us.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/es-us.js
MD5: 276e7c3c7756f9e962f6141f5048894d
SHA1: bab0d54cfa34f527dcf6960f5379aeef05cc66c8
SHA256:3923c6bd6137387d5edc62f6dc0174cc9eef8363238c16eef78bd9d9c69bfafc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: es.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/es.js
MD5: 0e92f45548e01672fc6a2f73979c397e

SHA1: 6e6385cb5f6e39ed9ba95ebc1fb66526e2c3371a
SHA256:2a8f1790d492fc338933a032a862f99998f31bcaf7a0e4fc298b6a3cb04cdf7e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: et.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/et.js
MD5: 8b5c6c8136c1bcb3dd35ff204c28b1fc
SHA1: 82ecebf743869c8231a6ef06cf5959e5cdbc7fc9
SHA256:95c974679dba419b7d835fa51340c430bd0066bdc38a7a139caa575b67389d7e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: eu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/eu.js
MD5: 1f0f32ac558d6bf2591f0e7c59b09e88
SHA1: e8989f9da9ff458c51d7d4c21f9bfc99ddcd72a7
SHA256:ecbc07cdb215cf9996405fa56ef306761ec6a9383e19a53c2b45d6a1c5c4dc68
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fa.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fa.js
MD5: bad9e9e51e7cd982360114a2d6b9a03a
SHA1: 7285494b159552cdee8bb7050d1278144da80b04
SHA256:15ca66ce1faa865c68998fcc8ab1160207636b9161ad76f7cf7acd0d7c0ebd1f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fi.js
MD5: 08d74def02ac724471fce607ab87f4af
SHA1: 7f40cb04e95803f706af5caf5a983f7aa3f2365b
SHA256:1339d4170019588a6764a56236c2a7c5b2389ace52a9ec5e8c09f1997935741f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fil.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fil.js
MD5: fbc9e6bd5b49897ba8503d27e2d061ec
SHA1: 2121d4a7333acb3b7b120c1580a809a8a5927dc6
SHA256:d24cac0d0069d89c48b4c8cee34cddcb7e39892c91f07b884574fe0cafb66ef7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fo.js
MD5: 85d4a1a25dd5c3fa021f9e6f63fd01ac
SHA1: 95d11e45e86f344a148706df7f5c86019e02ae30
SHA256:6338de573601e330030918569b8d2f80f98a57754e748a03ff56e3672fa25be7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fr-ca.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fr-ca.js
MD5: c0ef60f7029fe6ab773c090320f0a66e
SHA1: 8970ff163faa9c8702be24f65f95e94b962d8622
SHA256:59c5acfba5605fa641721bf16123300164ccc043f4bad6009aa8d880b159124a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fr-ch.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fr-ch.js
MD5: 3345c9d13645ae5fb2964c17559326f5
SHA1: d0cd4c6466797300434db0d6c8028bf46fe35bc0
SHA256:b32f50aa3d147ba5441d7728a45bce592125fd0a97117ca4b93b32c6393d847d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fr.js
MD5: 775f1eb59d6f597b1c398036002ae329

SHA1: e6f1741f5598b62a83bb071459d9e8cae4b3a127
SHA256:d87b4eb850bc7742c104557450d0a70d18a48a917335221af08d23850667523e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: fy.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/fy.js
MD5: a54d9827ca1a619a839a15c94b7893a0
SHA1: 66863e3aaff531e89e83acd8844ca87f8516cf38
SHA256:c33ae59d9a05aca0dbe86d74bff25eb44d04ee97b738034fcb72a21b73ec1cf1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ga.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ga.js
MD5: 264a960fc2850670387b1cc90dc29dbb
SHA1: ddd261054362b16567ba858afae968cf2380bb6c
SHA256:fc6d5d441553b23b5ebc3c79896499a093a3285f1e6134a680b8899b5cca4c86
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: gd.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/gd.js
MD5: 0f3b98fcc8a06995436819446130320f
SHA1: 0050fa33180aa1f35c739cecb397846bff7d24e4
SHA256:efa1d779f65671809a63f900479c69bed19c262f2fe7936076793bd13deda080
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: gl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/gl.js
MD5: 0d346a7ad989c39c04631e181056acb5
SHA1: 74c436284f15589fd53c9d4c090a4f75ff8376aa
SHA256:825e6fad55094c13118d2cada0b6c5945a97ea9b647686c2b00dc6980bea4608
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: gom-deva.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/gom-deva.js
MD5: 6d2091e4ba1b31399eb4f1f3d92acaa2
SHA1: 9e27b24c4f8ff43da0373ca75738e0322cc1bd77
SHA256:ff5ebf00d100f610caa956ea22c45584e34067f762c2e9811326d5903ccd819c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: gom-latn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/gom-latn.js
MD5: 45f0c567784f534e16f304dd625682ad
SHA1: fc4b281f7d57696decbf3bd5e8c572f4191c9289
SHA256:caa6b3cafb8d463c7cb0b47783b84d7f7637f685b8d33d1224548f7f9a124cd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: gu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/gu.js
MD5: e108958bf473fcc52349ecba7dcff10e
SHA1: 977667ee217d20d2ff2338dfa6ea9bda2e0c13d5
SHA256:5155f3aa5fe43b18c7b06cf02ff6e9d6c157d7da822c658fbd8e2f0edceef161
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: he.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/he.js
MD5: f5e7fb20bbb7618d95e4928fee094f7e
SHA1: cbcd69bf9fa2cc2493d086af3a5cb15e893c7d64
SHA256:93b540d4f1bc21d5668854475e8efd2d6fcaa2f596704752a586ce07d471d475
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: hi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/hi.js
MD5: 10451c28a31c032807f1fbf1bea5c32f

SHA1: 8ab3e8fd6823a63a2348cca98ca4eba215ad01a9
SHA256:482f9289851cc5add17895787d427259acf8d9467db37000d383021aa097a1e3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: hr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/hr.js
MD5: bfeb6da022ce8f5d4610a485f6063935
SHA1: 0e475a985f8f3612c397a07781933bc4235be646
SHA256:4af37cc6b498a4c3418f0b5d90efe5354422b3d158681454dc2eedee31ce1469
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: hu.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/hu.js
MD5: d485a763ba31196c55bafddc763cf98e
SHA1: 83c283112870db2a37b8d6a96e2ff423f27addac
SHA256:518c3c1b849d41be9ef9673726ac3c71290096a727ff29c9edfb0f7489e3253f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: hy-am.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/hy-am.js
MD5: 8fedcd99fde263a8a5a906b27de70605
SHA1: 3fbecec521a9f7cdbb7576fb37a3f35ba2705e88
SHA256:2c3bf5ef8c5162c7c4ed0ce4b144fad24eefd691911d7c8b86c21cab84f3bfe6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: id.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/id.js
MD5: 3000b8d8d73e16384fd2a13aa7259d3e
SHA1: 1bcd369482f53edce0c1d34aeb15a918f3c7af7c
SHA256:036154641aa4cba94ac8a65b98af75d2fa0ec29156674947d1148fa146689dc3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: is.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/is.js
MD5: 0f5a457d3457dfeb1c5d256436b5e442
SHA1: af0c0c6573bb9628ee8c97479651f65571d6a56e
SHA256:6943c853ee0ad65ad2e3e38baecc90dc8088071f10406ee8a5ad995d7cf5f6e6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: it-ch.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/it-ch.js
MD5: 0c0cd69247909aeca5d78d255b30a617
SHA1: 71631e4e4ce3a8466d80d4960a86605634a713dd
SHA256:9670e2244dd63556408fc20671fd763fb91be52041eee92934710e75e2b3b7fa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: it.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/it.js
MD5: 1abd9a8f32e7930bbdebd23a2bfa4afb
SHA1: 40cc21bf11475c48c1681ebc18a63a2bea4b8962
SHA256:2fe7346bd6fdf02aee19fde76bd2ca0b5e65903ddd45d097be2342ee7b0b9470
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ja.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ja.js
MD5: f39b4bc3b33715242a84fed53b50d596
SHA1: 8bebb66d25df95fc67d48f4ebc4b519fbc7d9482
SHA256:9720de4592dd94861f2fabb51110533fe44620f517e50448dd828a7f2eef7009
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: jv.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/jv.js
MD5: 307628de0dbfe42c1aedc98c3afc1aae

SHA1: 7620cfee82f0241100b34de89cefd40412456ef6
SHA256:707617feaac7459e5d5c39ff3ea4a5e5da0cf398384902c1cd5975cbd1a113cd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ka.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ka.js
MD5: 629be6bde33738ff66f7119b3b617798
SHA1: 02209d78bf7dfa3b5e585e64ebfc61ce561e5f3d
SHA256:2c15068d2ceb1f34e4b92f95710b181bd1034410b8a96ae15dd11ee24d0ff0fa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: kk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/kk.js
MD5: 4532f947979a50597d1c82a42f0facb8
SHA1: 9a8cad32d8e4350e40184813f4d19aa05882a8c9
SHA256:430c86f6c0ea0199d8622045883048b35875bea37b44424663bbe573056ec981
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: km.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/km.js
MD5: f73d0c92be21341d171e019c00173f3d
SHA1: 6adb747842bb733d90ce2b7dcf4963f1d62a7a4b
SHA256:01b837409a1ee03d8269886915f10ae1b9460b2cc42cc5f6fac862f7360ba103
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: kn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/kn.js
MD5: 72e237c519a91674447b268b61983bbe
SHA1: d72624462d7dbcf362ccc15385d5cb5a124304c2
SHA256:9673f6d7a10086cda8228f1c080ec032e8f34e3a3de2f1413582e0a6cc6f2128
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ko.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ko.js
MD5: 14369b837e9e15378938754b04bd2189
SHA1: 9c886434ef46530e25cea737272027ac505b6adc
SHA256:f15f592b5d7d5bbbd061c5ad31d4c45f462ad43acad74808c6a7105b108ec0eb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ku.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ku.js
MD5: ba513eb127fa22206ca1a67ad8467da2
SHA1: 45c0c079a209932f8a8be25a94f0fb97be8ebf84
SHA256:816c9c27f4237f1fa595c5be0a60b7e5c58ec0336d5a908e03f73fd8596e1caf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ky.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ky.js
MD5: 68f9c0556546367a8c25903bb8348b80
SHA1: 5bc99ba86f969c07cd1b0dc62510c572707adb64
SHA256:d3c35f2c47610c7c921268cb98cf398599068d24d51e7a89167707130c85ad59
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: lb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/lb.js
MD5: 474c1a2279d961b67a8329372fb54367
SHA1: c6acf49c446bb128ce8aa5f980664107e92523cd
SHA256:cecd52da4e3f3a7a69d4cde1692c90d000a3726772f8e00a9c232faf4d6ff985
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: lo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/lo.js
MD5: 629f0195acb5feb16432ffc78b6418d0

SHA1: 10730e85c79a5c325f30a5f0fd1b83928918cde2
SHA256:83c284d16d40e861cd01c28683acf77475813993b2a17201f17127e238e5bcd6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: locales.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/min/locales.js
MD5: 3aabc3a57ff7796110a9d427e6e61280
SHA1: 59155d41e1b7a2f651f26f8db2768c42206bc4b7
SHA256:a6d8d341af2a118463f8dbec697f3b5210552997ef51e0d9a77c84235f2eb2dd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: locales.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/min/locales.min.js
MD5: 5d62f0a64211c2d3e0d009cc69c48202
SHA1: 4c6bb9ae2e43259229cc16e9eb7ef70f3c8cea12
SHA256:1a3224b3cabca0fa92ca56e14da46d7f209ed28ce68ed50940b4fa6ed2ffd254
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: lt.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/lt.js
MD5: fc931f5db9a4d5b832e7c53985cfb233
SHA1: 6d5575d2ab06036bb29e50e7b4607985b0c10aec
SHA256:a02ce50203e4cc9e85db77632d41f489f14c893f986199c8dd04191199924094
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: lv.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/lv.js
MD5: bc6f1396c4b85e2b01b4b2fca550c0b7
SHA1: a18e4175ecd49b5e3382dac1bbcdc48c3279c60f
SHA256:e4f68dbe7147bdc76d7614102eb525f9a5d8dacc690dd661091412b0c9505cb1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: me.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/me.js
MD5: 4b76ccc2617dfc9bd6a54643659bec05
SHA1: 924aea795ae1a9581ed184b384806891ce336e27
SHA256:24103df1e95500b3fdc4aa60b933c66d2cf33aa4ff8d2401ae847c516285679e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: mi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/mi.js
MD5: 89179085b30d2752584c4f4e9c3ac04a
SHA1: dbf999f790c8e7f99c27c55d8184cb46d1f0ee85
SHA256:9cc67dce66cf3f0f9a57ce732af6878cc23fedcf256fd5302c6cf57df87eac3a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: mk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/mk.js
MD5: 7a6a2a4ae623481704f78bb0ed6e1968
SHA1: 3d984281f4acbb38920919c47916a0ecc46d8d82
SHA256:c38140b5408a91d9632765d23f4368f0cc98dfb6aafb0fcce452b6b4bfa93efd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ml.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ml.js
MD5: adaeaf5c9b5995567c7723ded581c647
SHA1: 3cbb01a59dbfdd3b86caf1b30938598c52e1dac8
SHA256:d45ac595a918393ae8f76838688fcd569c917b945e9c53861ec4a1f11f20aed2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: mn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/mn.js
MD5: 2229e9c27b35b688a4211bad4d7574eb

SHA1: 7fb0c3b04afb903aaa0a3a1b4b478a8b2d9d6bf3
SHA256:0f1f5bbc9eaf020931f8cb54ae085e51c41c0761ffc7fd265dbb60cbe7d84076
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: moment-with-locales.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/min/moment-with-locales.js
MD5: d07131713d356424c14481ed9e77ced2
SHA1: 6ef93c81041412f1b60d1254595cb04b53f8ec39
SHA256:f37cad4429c2815e53699ca98abd4e8773737f696fff554c63a58f4d6589200b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: moment-with-locales.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/min/moment-with-locales.min.js
MD5: d458b68730a7330653700489333a7837
SHA1: 4059aeca1d0b99aec8006b37a927f09d9c0e794d
SHA256:430725b95468277dcbccc27e08e3d873276c0082737310b0b1ad330392511847
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: moment.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/moment.js
MD5: 6e5aa6783efbeff584f4292398326b32
SHA1: 450696675b814c89ec016901b570c05891ca2c04
SHA256:c33f09a4e1230f3075be8d2a94081108d52f62d3c30b9a238941fe80790267c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: moment.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/min/moment.min.js
MD5: 6c0a2330b0d8d6ea185d4669a0eddeab
SHA1: d4f50308961144876b2b5fa57684b737694a4b04
SHA256:f343aa319a17a3fc372ee6ad5af482b9bf6a298cb22652b4aa7502604821071f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: mr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/mr.js
MD5: cd715ac0f919538bf79acdb4a477763e
SHA1: 467bc9f9b59ee399af6ef3f89886c150f74ae52a
SHA256:f6347f442281844a205245620f9e469f52cacb7dd41640ef67d32a94f2c583d0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ms-my.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ms-my.js
MD5: cb7a91cedb211e85abf06a4683d39800
SHA1: 05754f446f94d9b0d34885bdb0dd40d08df23295
SHA256:fa77f6b23884ace43199d189a596c8cd436ab20b2b6966599dd9fd589e51548f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ms.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ms.js
MD5: 3f2df63e4e8e99e5f3a23b44e135f90a
SHA1: 7e8563a8e513fb3f2f711395992fb34d6039e841
SHA256:6b6301d42544281a07e51e517a1acd2e498e6289b29e74817433a86751761f71
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: mt.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/mt.js
MD5: 3cc610e1a28bb045e3f21adfa96614ce
SHA1: f22377dc419295b8cf22ca6459df3f834475ddf9
SHA256:6af1d3643bd218941f30da0f6ba7bd64d4c2d0c49336876308af3af0387b0440
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: my.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/my.js
MD5: 1de06907d41a2fbf6861958ee0eaaba6

SHA1: 1b5eaf3d04d7a45a9e93db791963bfa0cf999383
SHA256:92732cb26a774bc3e049c7e212d8ef1425413d63522ccca1fb1b0696854da4ad
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: nb.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/nb.js
MD5: ee293037089769cbdbbf9f2dba3e01e6
SHA1: bfed5520bb401c83f0b391cf09ab1907e4362f2e
SHA256:36f088dce675389ff1b12afe35703b6d166cef8df8a24e1e1d6ecfcf7be84fd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ne.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ne.js
MD5: f09e1496b96096e594254145053e777d
SHA1: 601e6b5e8ead8fac21d661c4cb1f5aee22c96755
SHA256:804bbd6c30dc3b74de711a44f9019db06210323a0db31e53ce730feab5ea6275
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: nl-be.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/nl-be.js
MD5: e50c24ded5247900814470d1a6cc8854
SHA1: 73d12dfe3645a5ea9e0b6c4d5b2a5f28ac022af2
SHA256:2bd27e18811c7363a1b46b815173d626102523a2f76854792885166f4a99eb5f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: nl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/nl.js
MD5: 843085f588379356ba9556d93aa9ccdb
SHA1: afe70913fffce08e256c3c9ffe350272bcb791a0
SHA256:037e055b18b4376112d853e3d357b217dcc0bfd3990e0155b980ff622b4ff8d9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: nn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/nn.js
MD5: 7c29b42f21ff6b7e0b1f16ebb20d2a5a
SHA1: 9464502746665d34779fd3e7c9c05212db534556
SHA256:66007f84c945a3475100a3024d5fa3d430d6e11e64de81849e50ea73e3f390be
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: oc-lnc.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/oc-lnc.js
MD5: 16a8d7288d0007906a6ebb39fd954265
SHA1: 5442e9e7ee72e6f2ed438139d5779ddcfaaf471c
SHA256:1e03cd598c495e4dca3bae56e3822cacde57333ab5a85f555c582e104f54261c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: pa-in.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/pa-in.js
MD5: 8247ac1929cfdcc902a77542e9fa470c
SHA1: a0270710978d4f03b32a4d5cd38065d6d274729a
SHA256:5ba548ba7844a1c5c4a7f003337237f940b5e8aa67254fb90e1a05a66f2b43ac
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: package.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/package.js
MD5: a26087930b5278aa21fd79491b952ac0
SHA1: ea880b139fa5aad30129356d4c2b61c7acad7452
SHA256:6334f70497c6d8fd22adb3089eec30bf1e2b3dacf92508df52eaa7a8aee12bba
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: package.json

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/package.json
MD5: f1965dc95e9d5ef4816ffbb597d484ab

SHA1: fa7b033b3a1adcb85370480289e6a60cfd21ac89
SHA256:25f5d25a676dda5763fea169d93a31dc12bd0a6d5d7f352379c8afcb1e3d794e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: pl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/pl.js
MD5: ea2f9b5ff7c97f62603f1e8786708d7a
SHA1: a9b097f9c1dfe0872befdf47995602029bbd22c9
SHA256:5435a1265dacc269403f275095e24a63ff3b8bb0f95908f7a2a987fbe2ab9e43
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: pt-br.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/pt-br.js
MD5: b70a96c3353ca41f14b5628aaeef6461
SHA1: 02e3841b0ed1fbf086a5b8bc1be8cf835cc9d8c2
SHA256:8a8b165be42795d9e945e7494f38ea353ee2f7eee7eab123073f3a42ce755687
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: pt.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/pt.js
MD5: 71f120e6f7682b0e80a9d5982b8a4711
SHA1: 49494f7c1cdb36294b6d640a524c2cf19eed12b5
SHA256:89e4c2f2d351ad7e2fefec9332778b16cd4a31858ded9ad6fece12fd9db94ac2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ro.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ro.js
MD5: 84b1a53a794d8749061a53eb558110f3
SHA1: c2241e36357a248cdc870a8f83c19d12a031b479
SHA256:f66bcaadde14018ffb3bce26ea8ffc3ce36cc65c4c1e9ef9ed6cb321b7ae9481
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ru.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ru.js
MD5: c66d22693e1e950330471ed9de408aaa
SHA1: 3f4b2156029a26bc408cdfccf5812bd125c760cd
SHA256:47b9c98d906dcdc3d7b7f40e604d793fff2e142f7d788f6ac0deac5030458ef5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sd.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sd.js
MD5: 115132c218de16cbea034b2762b9df9d
SHA1: ff940a6362744a8258e15cb09c4e4b46c48f3ec9
SHA256:e5f27127927a41eb82e45491e52bd6a529d3db5e6cd519c48f7473268909f6c3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: se.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/se.js
MD5: d63f9c00eb2beeff26eabfea1406a3bc
SHA1: 8fc07d6276adf84ab94a1d352d55c105769f9017
SHA256:424ed10805d004f217b44ff6a0da5bad51d8f3b25577306f6e1f59c387525da2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: si.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/si.js
MD5: 0bdd326bd6fe7e94a1c3fed06cf79cdb
SHA1: 6dc83c8bee2af014c11994abd5f0718ed9c4dc64
SHA256:8e7582efb99ff00bb7aeb6de0bfa65792592a5b4e81ae6caa7bf8cd8cb3180de
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sk.js
MD5: 0d4c93cc1adf0c2fe5bdcde7b1cca213

SHA1: 17c72fd3b31573f097f962b851fc82db22f217c1
SHA256:7685c076b71fd8e36c2cb84c645bb3a75d84566f26c3682a2792f0113b4d9b16
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sl.js
MD5: 11bbdf40343f7ee615144b2c3df93d54
SHA1: 853a6dcfaa15df6205729d754739633de7e3f667
SHA256:ff2e8352962c2d13d114356c863701f2473651f6491639e1826ab417d0377f90
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sq.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sq.js
MD5: f5c6cad85947f97d184ce17397145e3c
SHA1: 1817cdeeb3261b7f03f13902a7d8adfe46c36a65
SHA256:9d7d061c245349d6897732c90ad57841c9132b9b556be07a24dc76ff17cf75a0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sr-cyrl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sr-cyrl.js
MD5: 403a704d0b31d44f5d43a05f060f879d
SHA1: fe545c0831b16a2393a771221f2daf3f8af50cf8
SHA256:e62567ebcb6434f8652b1867386d7324c06d1f226fe9fad0517e658503ab496a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sr.js
MD5: b5752681e826802ad4578a65d446d2ab
SHA1: 18c79b7064d378b578c83facf15be80314e34581
SHA256:307eb8be823a2997ce88c5ad8c3ca19e7a6345f116331fe3856659665de0d453
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ss.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ss.js
MD5: e61a001b0c3ea5bebde2d4d96d7c19c6
SHA1: a26e124883144d6ac990722d7915ceb80a44f7c8
SHA256:0d8a08574cc28602738aca72bed6364e88dd93fb2131a20c06630e3dd7565945
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sv.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sv.js
MD5: a276c85890a03d5a55715768969516fc
SHA1: 135396ef7e63b71af3df1cbafc5b060a32aaea4e
SHA256:08f8dbba970b89522adaabe609f47a3f20857c0985967888124f9204f4c3e2f0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: sw.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/sw.js
MD5: b9e0ae98f621d6f9a622fe09225978cf
SHA1: 42f76f09c8d7049758fcf8f78e30881e6681c40e
SHA256:d6056ac79071a9f60793825357dac3ecf35c43acf10e02a65f1892f1fd9cc0c1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ta.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ta.js
MD5: 2b48e3a057ec1ecf49d4e16d56263ed8
SHA1: 94a700dff6eda352ad3a2c4d7f5a4dc5e6219321
SHA256:2dae88a3138adda69fdec54914461ec28d4fa5e720d7626ddb3fb91a74a2ab6b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: te.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/te.js
MD5: 39e36c17c46798dfdcf0ddae92610807

SHA1: 1168038e9d7c735ac44fc0eca95796067ca7b51b
SHA256:2cc07292a2ab5702d8e1e849ae3b28cca5c6194d0d150ec637c6289d9d864e32
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tests.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/min/tests.js
MD5: d39f31787b27fc1bb028ef80e699cd7c
SHA1: 4c0335c7f8c19e26ecdd2f9f0ed08323507031d7
SHA256:895d3ab9bb945f1f86903438a18c9fb308e84a912e4859da39fd1bb08da63e44
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tet.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tet.js
MD5: 0a6f7fbd649b280c8fff433d32591867
SHA1: 15f108397be93776a1c232f3de813e27f305550e
SHA256:d80dcb236c671594af031c93d32ed883c322a6f32bd25637d454d7b9d9e81593
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tg.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tg.js
MD5: 83e93f32f7f488c26def6938e280b716
SHA1: 59886e50e9d7e53beb111b317d5195ee0382050e
SHA256:24c8928619c471831467afc05aca6f0299e40b418b78bb30b4d66942d872d2bb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: th.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/th.js
MD5: e14a3488b2c85b54f65262d6fcc6b1b5
SHA1: 7697e04cbe08eefdc5ad4cefca7ea7ef42cac791
SHA256:9911634c353a7ce63a81139f914552fc80a499029a803ced8b32b6af88c53bf4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tk.js
MD5: c01b5d264b1cfa34c4723e995439ebb9
SHA1: 8445ede8c1ce77556495f9a5469ead5d3b2b3ee8
SHA256:fc6654229cf3f6e6bb2aeb5b70dc4e6adf7f307575af9d15b7a31aab897a9988
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tl-ph.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tl-ph.js
MD5: aefa584c5d3e7690a710b144fc505a7d
SHA1: ccc8535e56aeb0b2c2991ec7c2c232a16334f09b
SHA256:e324f1791432534af3ada36c185637db02eaf3d3ed8f88ddf143538dc484cc3a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tlh.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tlh.js
MD5: 59508c37879615bd0a0beee8f69a28da
SHA1: 15324b9edf1a3e7bbc52b1e510ac53def8ce02ef
SHA256:dccea1319a2e92d9bf373e1d8dadcd4a130e1fa2457d7a66dd035c3cb93601cd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tr.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tr.js
MD5: 0cf5765f4f245b2cd8a21dee0c3c92ba
SHA1: 7eb8afffa83fb85eba987c80a934c6ad30a23b23
SHA256:e8af125b0bdb3c15ff5ef2eb171bfe698507a026a9cab54bedb0770cdca34fb2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tzl.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tzl.js
MD5: a2587bce05b5fa3015dce4ccedbdc802

SHA1: b9c4bb7a9f9ad9dd515bb9de82be90d0d4932fe6
SHA256:393e6424d498fd2abbf646217a197b61c4c57706e6b29ec2873ab20e7bdf6970
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tzm-latn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tzm-latn.js
MD5: 582198d314e9ced1007620d4e7701734
SHA1: 17859d3345ae82ce39d5d036649c1976b9e4474a
SHA256:7909cef0eb3080599c24794c079e05ba07af565f198450df0ad411c85be45030
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: tzm.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/tzm.js
MD5: 69d71f7f7674fd7f8b35f14dc179339b
SHA1: b5166e0443eb54c38185227e954cd5cc2b1f589b
SHA256:e6f3a2e2e3ca86953e2c06ca562607a95d2b5129e751e5e0905270f3e56a1f52
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ug-cn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ug-cn.js
MD5: aad8845e8fb63517d21b322fef4a3545
SHA1: aff6b2361311a6475b9fd755bf63d23e3e6132b1
SHA256:58de2ad653876b1eb27ceaffb0037ddb0e4fb7917e111fa7a88ef8ab01fd041d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: uk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/uk.js
MD5: fbe69f339b236b654b3e41d8d8b56536
SHA1: d9fdc9224f535c1338048858a9e457558f95349e
SHA256:725764b2851d3db79d8fb20b96ce7708cd1dc60c6ca6f37bac4df2350f3ccbf4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: ur.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/ur.js
MD5: 3da7117995350068016398429 5abe43d
SHA1: 2fdee5b33f8d29a565d84927fd333a2d9d41e5b2
SHA256:c89fc485a14cb20c0576ff20bc3d157e1296f2b2ddfa8035f71e8b58f61a29a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: uz-latn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/uz-latn.js
MD5: 75ce0ce4c28806c32575c4f28ded6185
SHA1: 2648a6adc3ebb4dc12b070a5cc0a126050cf685a
SHA256:3943e946fcad9c965f147c50e08da71d3270239175de530d1f48be6fb44956ed
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: uz.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/uz.js
MD5: 3d11efeaad9c7b7f344eb8beb691a2d3
SHA1: 73ce197519648ecb5e6756bb2fb953688b42af2a
SHA256:9f22344f9ff69b1cf5546c975fd8847884bb032216d15054ea267cb964a09b08
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: vi.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/vi.js
MD5: 28c7ec0c4bf82120245da0d15112f4b0
SHA1: 1470d1969733e49331f2e435910b045e6a0a518b
SHA256:c5db03ae438e4c55a6edfa004540aaf1def14fe0968f9ed3e03fe7dd7c3faf03
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: webjars-requirejs.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/webjars-requirejs.js
MD5: 34b1a7dcca0ee03eed1432670ed9c472

SHA1: 9de80e951270f04bbafd39d9d7822df4f7d08839
SHA256:197295e6af66b25f2aaa0909c6911f7c1c76e24eaf170d9cba2d84644146bfeb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: x-pseudo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/x-pseudo.js
MD5: 18b5b8d8f2f327f6d5ec947e550f35e0
SHA1: acc470244b95f709e4b68e7ab94b2c645f929f47
SHA256:ca8ab052a09b2f320574c71c472609e026b4aa72c87a06f204ff33670249e2bf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: yo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/yo.js
MD5: 42b28f7a2ea67c7b5a342c87ef0a5771
SHA1: 84f6d714e3aadf74ab8a755b465df7ec8215fada
SHA256:d80655b604558af2855f5b67b21b28ec5770985b67fde59e94e1168e5f4795c8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: zh-cn.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/zh-cn.js
MD5: 49fa27dd7c374122f336369f30a87973
SHA1: 768eeb42e5372200634e8825680c6e18b0c8db8d
SHA256:53138532aad7c571af10cf6b17a678552e9a9e7ef5014d250f97af8dc61ae6e1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: zh-hk.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/zh-hk.js
MD5: 9338eb6ad8e887a63be4fbaa05cab197
SHA1: 92340e4f48872df241a47bf9bd13647092fd25c9
SHA256:c6d7de0d1f5544a1d3bb64c7eb27481b30316766f1214fbb5b1c6be358a4b921
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: zh-mo.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/zh-mo.js
MD5: a986f68bda18d9751f6bedd7356e6e7c
SHA1: 6cac0e5b7b9e15ea799ce6a1575be93df4832c87
SHA256:874ca3806f556c5809842613ba410c965111ea9441fb949a32abe2a7c3bf7f8a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: momentjs.jar: zh-tw.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/momentjs.jar/META-INF/resources/webjars/momentjs/2.29.4/locale/zh-tw.js
MD5: 94fb46a7c1ce21f0a91512b170d4fdea
SHA1: cb69c6ca687ace454432d994ae5b624ba9011b62
SHA256:62fb1b36d24050120cadf807b975ffe9d7986aeb41a0f4ac218c3ad23a1c9b1a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar
MD5: 23c5a99b63417f6dab611b9bde066852
SHA1: 7a473b01561d0cbb0c36755a1d9ded53a0ed340a
SHA256:96b158110632a551eae8da4d484b5918c4833a4a76869836bfaa40d131da1c4f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	remotegui	High
Vendor	jar	package name	gui	Low
Vendor	jar	package name	inet	Low
Vendor	jar	package name	remote	Low
Vendor	Manifest	built-date	2026-09-28 17:03	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	remotegui	High
Product	jar	package name	gui	Low
Product	jar	package name	remote	Low
Product	jar	package name	shared	Highest
Product	Manifest	built-date	2026-09-28 17:03	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	remotegui	High
Product	Manifest	specification-title	remotegui	Medium
Version	jar	package name	shared	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

remotegui.zip: remotegui.jar: angular-websocket.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/lib/angularwebsocket/angular-websocket.js
MD5: 40cf028986784d5006d57219f6dbe0a8
SHA1: 40efa9ba93f90c2933ea22c767a0b1439e10303d
SHA256:eb77f7788e6b757192f2fbf8c6af6560731c3539b06fdf7d476e92b989ca50b0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: app.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/template/js/app.js
MD5: 6f61e39f7ed0928ce2046d44760db061
SHA1: 1a79dd0d084db06894770d115b3b808a0d8c0ecb
SHA256:bd0c38131628418202bc8a896fceee79fc4933ac37da60263562ddb37ede2f26
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: app.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/login/js/app.js
MD5: d9a96ed732439b0dc0417d960d30b667
SHA1: a7b2247fb71c27e9eacc8f24859fb993be8d95d1
SHA256:49b24b3125429b20e816a2082e45f104ac09590c64d61ad8d4fb5c86cbe83a93
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Related Dependencies

- remotegui.zip: remotegui.jar: app.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/logout/js/app.js
  - MD5: d9a96ed732439b0dc0417d960d30b667
  - SHA1: a7b2247fb71c27e9eacc8f24859fb993be8d95d1
  - SHA256: 49b24b3125429b20e816a2082e45f104ac09590c64d61ad8d4fb5c86cbe83a93
- remotegui.zip: remotegui.jar: app.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/masterlogin/js/app.js
  - MD5: d9a96ed732439b0dc0417d960d30b667
  - SHA1: a7b2247fb71c27e9eacc8f24859fb993be8d95d1
  - SHA256: 49b24b3125429b20e816a2082e45f104ac09590c64d61ad8d4fb5c86cbe83a93
- remotegui.zip: remotegui.jar: app.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/passwordreset/js/app.js
  - MD5: d9a96ed732439b0dc0417d960d30b667
  - SHA1: a7b2247fb71c27e9eacc8f24859fb993be8d95d1
  - SHA256: 49b24b3125429b20e816a2082e45f104ac09590c64d61ad8d4fb5c86cbe83a93
- remotegui.zip: remotegui.jar: app.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/signup/js/app.js
  - MD5: d9a96ed732439b0dc0417d960d30b667
  - SHA1: a7b2247fb71c27e9eacc8f24859fb993be8d95d1
  - SHA256: 49b24b3125429b20e816a2082e45f104ac09590c64d61ad8d4fb5c86cbe83a93
- remotegui.zip: remotegui.jar: app.js
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/signupbasic/js/app.js
  - MD5: d9a96ed732439b0dc0417d960d30b667
  - SHA1: a7b2247fb71c27e9eacc8f24859fb993be8d95d1
  - SHA256: 49b24b3125429b20e816a2082e45f104ac09590c64d61ad8d4fb5c86cbe83a93

Identifiers

- **None**

remotegui.zip: remotegui.jar: app.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/reporterror/js/app.js
MD5: 6ad83588ff8ae2fca8a22a9973c9a22e
SHA1: e34a66c038feb5d7eaaebe6f5641ff754ba2133a
SHA256:171ea457d3942a068d637c9c416f4314d2e337896c4c06466d5048d1b207964c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: app.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/start/js/app.js
MD5: a92b24ddb292c48b2b37f8f612dcf510
SHA1: 4fb6c8ec1c639068e82cea773e346402bee5db6b
SHA256:f9a5dfaf43cc245a92f3da0e6a6a05df73027571f820767630c897274510e125
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: appbadge.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/appbadge.service.js

MD5: 4fd729dbd4e3e172e18625eeeb1d21f3
SHA1: bda842fc94e89b87c8ac7ab1fda990058708c679
SHA256:8ba199a5047196dec59a090d09d62628d962bd4827c6f58491688405af98bf20
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: authInterceptor.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/authInterceptor.service.js
MD5: 7fa3864d221a30bc7380c1d61fd0127d
SHA1: 7711e764bb81e7518be8f1582ba36c0bcaffbc12
SHA256:78a5ae26f5463a9ffaa3aba943dcc4a6852dafea4e6a161a77db4e57e57c9565
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: avatarcard.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/avatarcard.directive.js
MD5: d3d063fdda23fd7b8254230bf8475278
SHA1: 5d13354507fd7d88bd4abeec4221adbfc7a016b3
SHA256:5e3a3c7d0cd3f8e7e0b0e0f5b808564575a348f859ef850b02c004c6baed1f8a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: avatardetails.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/avatardetails.directive.js
MD5: 1736536ca17f8949cfbcea3546666700
SHA1: c6d2b53e9caa1ad5b19f0063a4c7f88c31784ccc
SHA256:5bedc4c3e7b3be6a29f2c85fbd2881b935f24172fd42d5f893f221c1972bdc5e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: avatarimage.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/avatarimage.directive.js
MD5: 70e2255c02822aec0a74da3386baa781
SHA1: 927e3a72f635deb32b6dd3bd1e3deea711b73521
SHA256:9c3a64b8c4c5e6bdeadd27b840e1835d240e7e291b2499e331545d0f3d6fb3da
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: avatarimagedetails.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/avatarimagedetails.directive.js
MD5: 30a2af71a10ee42a8e840c52dc445a33
SHA1: 2767a8c4d10f738a7cbc2f0166473a721724465c
SHA256:4c5603e04daff5cb4de37b3a8e120e0049036ea10683980c3062c96919d1521e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: basic.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/basic.js
MD5: 1102f35b31d7756109efaa76bb21844d
SHA1: e2dac85cac0350e24415cc038d94de99aa012239
SHA256:08067b0f67b15ad273de6394c1d10d13c393c1d48a2cd9771990a948d6126e8d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: bootstrap-colorpicker.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/colorpicker/bootstrap-colorpicker.js
MD5: 66fc7adafdfc312da33c1610ddb02650
SHA1: c0fe35fdc3e1a7b23415601264ee3f5f8b6408ba
SHA256:359ac587e9aac88dcb26774fea01a3b04b89ff8f8d49c36b0dffd82d0ca3f2a9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: bootstrap-datetimepicker.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/datetimepicker/js/bootstrap-datetimepicker.js
MD5: f99cb51a76e41db0a93720a7ab76f79a
SHA1: 811d10b8029074990b4328164ea5645759789a5e
SHA256:3ae825ea00eae0f2169e66d6574fa1e8323b51bf253091bb5a66df76663d37ef
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: browsercheck.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/browsercheck.js
MD5: ed1d82ddcb85e5003c15d383c7547c00
SHA1: 0096503446b3e2ce066b74011723be1bef1526d4

SHA256:d86fea84c84f819be166f9519bfe84b11ebe3df812f9c6ae20d4edd57c077330
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: changeavatar.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/changeavatar/changeavatar.js
MD5: 4ec995f8f48cb5788d1c0ada240b452b
SHA1: 8a32c77a3ba19e018ceeffb30d23b6e7d723ca5f
SHA256:373bf0209751ede6dab59fc52027eee6cbf0c22799d3c542095294167bbe1928
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: changeavatarcontroller.controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/changeavatar/changeavatarcontroller.controller.js
MD5: 8b89fc5e22e1934967141c4f587147c2
SHA1: 868ff2f7879c4779110bd5a485a621b071f9a743
SHA256:308d3cfc40b3b8be525b7968cd0db33ca1b8125c1b8f7b0ce6589d0f0d50c2bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: changeavatarservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/changeavatar/changeavatarservice.service.js
MD5: a6675aa6f069ce9bbace3703e9eda21a
SHA1: 391861c018f4dc7af40c43095c8cd321a572f127
SHA256:eb25d9039b156b8e7b25512782f79019618e9b053a012611964411fd4fc97436
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: chooser-color-popup.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/chooser-color-popup.js
MD5: 139be815118c397fc203345e0979edd5
SHA1: bf982e3ebf6b05e1ff86090650fc010079f5d920
SHA256:05b039aa3dc832f169d7850470c6010b8f9c865e9c92a182754479d2a6fe2f25
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: clearreports.controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/template/js/clearreports.controller.js
MD5: 3a539076e4fbf0d5347b96e1e6cac2aa
SHA1: ee16a8d5998df2c3982a7fc44fccf4cf67cd57d7
SHA256:d823c84e44c8b07a5d64bad6beae795ef365da5cb01da5364e516d1d2caa6f45
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: clipboardservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/clipboardservice.js
MD5: 4e1e6b5bbd0964d0b63238792ed499a6
SHA1: cbd4f6c73a66c379830b7d39db2d5b719a145166
SHA256:5aef981c32fe1ca7fe038ce1247b842ab70d9b5b84efcf6805d9c7a9cef14730
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: collapse.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/collapse.directive.js
MD5: c1382e5bab1e0095998e5b19ac91f381
SHA1: 2bfacf81cdcbdbc9919f24433ada8d3d78ff826a
SHA256:f09aeeb80d0d0811b4e6c9ae46d2a975cfa372d339236dc1f74e238218a60be4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: colorPicker.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/colorPicker.directive.js
MD5: 21ef7608799862ae50c2c74f78d0a9fc
SHA1: 747b3d2b2615c51fda36d4177ff6742a3f254784
SHA256:ecdde453424a6164c70d2a8ae42bbd0e2f36aa424dda81a021daddfc3be97cda
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: colorservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/colorservice.js
MD5: ed1597fdebf45205570751415184d577
SHA1: 037de30d76e654aa6887f9dd439b2e99cace8636
SHA256:a6d46d65712c859c7bfbec04925c1edbe1d679cb10683b9463b8f1cfe1d74dee
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: connectionstate.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/connectionstate.js
MD5: 4a6174bd421f26ebbcfee0cd497cb818
SHA1: dd1fd437528d6680073b6ec992627e58a7117d1d
SHA256:4b755f8f5c4c823a55df73cda77ecfaad11829b5945c0f60e9c3be0de7ffcaee
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/template/js/controller.js
MD5: 06cebd797eaf41917ad90bccf3eb1b18
SHA1: 5dc73d85c4fbebc109bef054e09a26b938390b34
SHA256:15bd28be21d81cbfa0ab273eed67fd1d89b580252a756dfc52e14c3cb0f968c3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/invalidlicense/js/controller.js
MD5: ca1979cf2df78c9a22c96f3478247107
SHA1: 6b8bd8aa94a41d55d9b5c11f37a6e0a2a25a5a5e
SHA256:2e689b5bdc728198ed225e4e7634d0bc374f6d5f0190f706808d3c1857b1591c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/vetomessage/js/controller.js
MD5: b3d1cbd2470d7a37317a1a3b2f731b76
SHA1: 8be451bf390bbc31e274d966fa238675d192598d
SHA256:d478572d76089fa663779be7fb47933ca9c7bec7f97ada36dd8d7ca80f6f4eb5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllerAbout.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/about/controllerAbout.js
MD5: 80b4da64ffededbe3c3523b55e2bf326
SHA1: df84d88eb510b8e820880297404310f5a8795f4f
SHA256:48bbb094dfff3f6b7dcf787d12214c26dafedc27cd37003b651e1ce179026029
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllerShortcuts.controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/shortcuts/controllerShortcuts.controller.js
MD5: 9be25409fea8e060b32a3ed16afa0496
SHA1: 36808df213a842d807c44b517fcdabd52c7479ac
SHA256:18169a2a57beb8edc203674e334cd2eccaf262635e4cea0b408e2f8608338008
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllerUserTheme.controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular

/weblib/inet/js/usertheme/controllerUserTheme.controller.js
MD5: 3f22da2a31a50aae9eca2ddf181a32e6
SHA1: 92ef56f938fd823a8d2d234190af4aff18ce8223
SHA256:e3b5b9c6ba45a9f4e7ea82817ad2e4eebfa514eb88f0056ed61741a37917049a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/login/js/controllers.js
MD5: a8ac2709cc86b403df12e2112b1c50da
SHA1: 344a480dca6074c311786b03a13aeaff5cfb58a3
SHA256:3efd28cc6f37f33f4c99fcd534349933d13c07cfbb85ae6b424c7d0889e968fc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/logout/js/controllers.js
MD5: 72df17aceff55a08379e0d53b414a348
SHA1: e3364d95d630e8ee2831c6f8c043e380892303de
SHA256:fde8f9a6bd901c3a4fb1eff6e1b28cd70ed29ecd1ca0eb4d516fe8257b10866d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/masterlogin/js/controllers.js
MD5: b7ce1065cd78fdac56af02a9c2990479
SHA1: bb6e0f303c2a2601864542d89f2e2f5da4cc582d
SHA256:b062b60f3c71cca9147df8429acfeaf1333646ebed0a49abfd57e828594969bd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/passwordreset/js/controllers.js
MD5: 4dbf4bd5e209bcf9da2dbea374055b93
SHA1: 87bc7d80e618d023de04a942c4bcf78a0f63ef94
SHA256:c4fc820510883428e8b7f8cc620917ad024a053406fc8e06a1f5d291e7cb8277
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/reporterror/js/controllers.js
MD5: f0eae135a9846e9583286cd7e26e16c1
SHA1: 2ebb1635a8de2bf5a5b733d22be21e702b12b72c
SHA256:03bece9cc5a2def46cb9af89cf57416e825bc861f4bef8e388418e2e2f7fd2fe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/signup/js/controllers.js
MD5: 258465212e0911f69571bb053df33a43
SHA1: 91a7f8521507ac4c7f3694cf5dd955417828e559
SHA256:f3cd796047cab32758bcd5425fddda63249ccf268422094f9bafb9183d52a13b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/signupbasic/js/controllers.js
MD5: 17128560e8941aedb7e852204f4a179f
SHA1: bafe38ec75526c6f24a08468efcb54b174af8a12
SHA256:c86e24d128397562391debe2cda9c5a59382ed887ce040fdd950fba13307b093
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: controllers.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/start/js/controllers.js
MD5: 3451d3dc4466d917bdaaeca802ffedae
SHA1: cf35aaaad9461c21764024842d788d1fffdd36bd
SHA256:81ee322dec22a872c1c1b2cbdeb032036fb825c53bb8d0fee0270318ed49dae1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: currencyNumber.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/currencyNumber.directive.js
MD5: baae690d1879d5770a785db43c416078

SHA1: 6652a3fc50dbfeff6d2c3ba5d163b6198d48952a
SHA256:c6cf472a9ba060122120b728e7f034a46b42e3b035ef56144ff482bfe5092cf4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: currencyValidator.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/currencyValidator.directive.js
MD5: 73a660a1b69b3c877a80104908dcd0fe
SHA1: f452a6e6a90eafec046f8364e92e8991639fc0e3
SHA256:a54b14192bdf0b13eb46a513c0de90d2217df002a87b69faff4a97a2b438e78a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: customEmojiUploadConfigItemRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/emoji/customEmojiUploadConfigItemRenderer.directive.js
MD5: 614bca272bedcbaa6f867d223c67ca6b
SHA1: 158169ab1d6de578cf3d3157b44fc5568a0dff9d
SHA256:38d245ad840d4d01acece7fb531bfaf683e40367b70e1965761df25378601795
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: customEmojiUploadConfigRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/emoji/customEmojiUploadConfigRenderer.directive.js
MD5: 646c45383035b8a172b1e3cea4462065
SHA1: ccd25b4652f738ffd5db41da6f2c01b9bf2e8fdc
SHA256:366ac5823f773c9420495a3f7ccebc31703515e7840963340d9b088a9a280b8c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: customemojiupload.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/emoji/customemojiupload.js
MD5: 5ab9bc583256cb4bf16a2ed2611a694c
SHA1: 8aa95d9a6f7aa446ca449dd06a22ec766e011c3e
SHA256:10c1b4c00e9ea48d9216001bfde435ad3d978dc7924328afcde5985e31cc5052
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: dataservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/dataservice.js
MD5: e296e216ec8019aba19de9e5c38f6cfa
SHA1: 87f076c645b06b4b0a6f98f23a08d6893a759b2e
SHA256:1f1ababff3d0b755cbce83a36ea6c2207e131cb11df2d511e30cf8c9f4303371
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: dataservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/dataservice.service.js
MD5: 97eb43dbb39b2e8032f7c6704ee61467
SHA1: 1e7b131c598907d8060951dc00ff195c089bb670
SHA256:01b212d6034dc0c32cada3dade9da19b2730dc713c57b95589eb2ee15e7a9eff
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: datepicker-de.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/lib/jquery/i18n/datepicker-de.js
MD5: 797fabcb912b0290ab3e259ffab24855
SHA1: 46bdb9bae4acf4a0f014121d0f9eaf2d5c15cc63
SHA256:1bd259fc9bb5d2965296710ef6ea072f59c2ad669173e47958f672d0ee98de1f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: debug.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/debug.directive.js
MD5: af5e64405e9df914078db9c21e2d6cd2
SHA1: 9daecb829ec4ef49f5ff9415f03c1130b97cdfa9
SHA256:7e8f60d4320fb77c329b93858e2cb2435b756cc939395dcb0259f9324667cb25
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: dialogservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/dialogservice.service.js
MD5: e63e5787e78517515c545ae644786f88

SHA1: 88691106334ac503cbaab986eedfd6807f55f57f
SHA256:e5a253388ac6fad6a7b08237a09f561272016481509c850d540f7e9834ed8c82
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: directives.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/directives.js
MD5: 19f28ec5f19f91bee0b1c9e74e173dc1
SHA1: 8f3d5294a051eabba98d8b9ceada4b2411210e58
SHA256:0543ab08833d1e44de5f6c23d230703cea6ad2cb637577549e308d185afea1fb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: dropdown.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/dropdown.directive.js
MD5: 34a62e5850a9c548493cfacae2971677
SHA1: 72304276999b43f29dd0ba3cd13829e7208c6d65
SHA256:575b84426322c7c3724e5aac3bdacee5d92bcd2ddaecb017ff9bad91e1a714b9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: emojiModel.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/emoji/emojiModel.service.js
MD5: 38564647d31b6797536db5765411e4ed
SHA1: 48fd70c8edf0adcf125823e861e4a139a381cbcf
SHA256:d22736cdec4e2e645ac67859b8dd33c6af37c304f60a2d1da1d4faefb33f087e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: emojiselector.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/emoji/emojiselector.directive.js
MD5: cf4481407a72642bb8f659e8b1811a6d
SHA1: f5b4d06097e39d132c2e341005a5f37945e6d25b
SHA256:c9b023b87ba265d2fbc5af9dfaf4d739f2a5445ba1368d9fdf02f7cc0e07e307
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: env.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/env.js
MD5: a9a6e6f0910acb437990f717d4c5285f
SHA1: b00fca58e7a3522bf6178a4a97f2af761e55b7f5
SHA256:864170a7078a5e252286424d4d4d58a226ee0e70a43d084bb89d8ff0624d9f3acc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: errorservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/errorservice.js
MD5: 0b417819bafb4ba2ef637d2d33b359ac
SHA1: 37a9a05422c4eb6fc45036a72bf41d62babc6eb9
SHA256:cfe3685d68219b63688e6e91b225435695b1dc71abb6aea96082582decf0fa4f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: errorservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/errorservice.service.js
MD5: 8b066e62a78e7160d53be4c4fdab8611
SHA1: 2c2121db84b69116f40c058f601845afc1124349
SHA256:a10e2492e86f11e1d16fb3140d10183d394b4e4bc761588c6cf6fdfedac5e58c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: eventemitter.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/eventemitter.js
MD5: 2d07d566045034806abf625eefe74307
SHA1: 16be87f1a1804e7ec3ccbac3d6425212d05d333f
SHA256:88de7415972e9975a760a270534d959239d752497ad894c6b495389626a934ce
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: filechooser.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/filechooser.service.js
MD5: a165d81e282a2c075d15dadecf6fc3ab

SHA1: 7cb31162d3d7ab8fa80b195e60cc19924228347b
SHA256:7ca52a4f1e092c18509577c333d3ba9d84e069237202721244d5241b098d4c56
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: filechooserservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/filechooserservice.js
MD5: e81bf6e741ffb26878591b3e481eda1d
SHA1: 8ac847dfe8b64f26e890f7a03e2cacc2cbd38c5b
SHA256:dccb91f52258acbd53c4902c236597c33687542ee00c82a72be1a9c5252daa3c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: fixNumber.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/fixNumber.directive.js
MD5: 4012901ce3b8c0dd2c30de58b4010f93
SHA1: 2f74672bcb93cbc5a5ad537ab900e5ea2993244c
SHA256:df68e84e582a52b12400fdbc1ef79d935013e189579795a435a6ed8055573c35
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: fixNumberValidator.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/fixNumberValidator.directive.js
MD5: cd63efa13934af29deb8ebaa34d99d16
SHA1: 6b6c6bb19f785f4cddf2aced9381c3578a3213f5
SHA256:8d6e9515be7e1db5f56dfe91a1e96c91b8ca536f4ffdc31614a30a5a7e7dad88
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: floatNumber.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/floatNumber.directive.js
MD5: 0b5378d3a8d7f79543eefb43bd125bcb
SHA1: 0c50d5b03526ee6a4b5ecafca50e139183e64bf6
SHA256:e1e487d744826c96b46a8e946a32892ee07520f3f29e421d243df51291f729f6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: floatNumberValidator.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/floatNumberValidator.directive.js
MD5: cf0422e6f9e9d1503247ff475d10d3d2
SHA1: c0d2a9c1ba8905a8853b7880e484fd2546bd91cc
SHA256:f64676d8ca0e5be8cdbcdce1658d71f18608aeee7229a43e8076139ddf5d7f15
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: globalactionservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/globalactionservice.service.js
MD5: 6d4f2194f51d48cc3b21f9526f7fee57
SHA1: 30f480f24b629a9dd3a93fe04dca7eb04a20b677
SHA256:8c1f6dd7a7ecd6472d75748edd38d98783b20e103c898220b2e3b25f4090f6a2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: guid.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/guid.js
MD5: efe9abb6d7be1e4185b69d4c4b3bf31d
SHA1: 760987f1cb1537a0f717d985537da6c01ddd4577
SHA256:d734566d2b0d9d89e73cc0c2ad503d73141ef79a99c75139d5fbc207a6663394
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hdField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/hdField.directive.js
MD5: a693a2774b78373202304d2d9d5ac06f
SHA1: ea7b76c396bb2753deedc6663998c77f32aa201e
SHA256:31226a6c2b7a11867fd336efe0597a8facb11ea21a28f1911be1807430d2ac4f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hdMandatory.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/hdMandatory.directive.js
MD5: 5ebb609350c6d0ae645e8ac20cbb32b9
SHA1: 15bb7b61dcc2a479beee7e0162796788565fafc4
SHA256:593ebe1d558142ea9e12a998fba8034c5539267794d3f1ae01fa61cc30103e2d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hdNeedchange.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/hdNeedchange.directive.js
MD5: c3abe040e55d2f09b03b6ff4a839b795
SHA1: 4ba516326ef10cdbac82bfeca2ef5a82122c27b9
SHA256:49e8d8b1fe5a2d491a81412531fe794b9b32dccad6536f9b06041e7931f83a8b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hdValidate.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/hdValidate.directive.js
MD5: e6e8c3e26ad3be54df16ec1bb887bb70
SHA1: 4b1e88e7eed9dade1052f00086c2c09f18a0be32
SHA256:18040f9661212ce2406d973b0431fd3c320033bd4d6b931db124aeca515873f1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hdattachment.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/hdattachment.js
MD5: 16e85502191f7fe25433de5ad6c746f9
SHA1: 712909937e6a4ad47396146d4e79e4a3dd0b32e4
SHA256:b59d7f8b2225790fa30812d87d012f6668ecf1ce2d3a0cba04d987812ad2cd4b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hdfileupload.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/hdfileupload.js
MD5: 75a66761b717a6997b593736a3636c7f
SHA1: c7dcef33b520474109257a31e81c13967de4fd70
SHA256:1e85e4d3ca53baf4a8da1008aaaf7bf0b048d078a08e8bae3fa8628804dbe5b4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: helpservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/helpservice.js
MD5: 8c62a54227757b01b0f60d7ca811a270
SHA1: 963edb75fa6682082979958c1f0b667d530c84dd
SHA256:334ef438ffce3ca6d6449195516553d5d55ddc8d37d8de6eea8780fc710c399f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hsimp.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/hsimp/js/hsimp.min.js
MD5: 31da02c3356fe92d686f09c9e9a2d3b5
SHA1: 77c9d1aae30a77bb4f4ff1015d9886a9fb2bad93
SHA256:44cdb7ca377e6793dac301775332a628e89b3624b6330964a9e2592d1f5b0389
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: hsimp.renderer.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/hsimp/js/hsimp.renderer.js
MD5: 5f06f676ed65e93315ba629f480077b0
SHA1: 213a052ff56e4e0cce58b108a93995300b7f21b7
SHA256:a6741fb1ac97dd1d59dcbfb635c018a4fc51ee6bcbecf8f0928fb76019cf3658
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: html5modeurls.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/template/js/html5modeurls.js
MD5: 784c54f58e8351e6821785bdeaa852fd
SHA1: 945f8e892ff235c347b61d726cbca71c51cfa0ec
SHA256:3cb5e8d76193fd52fe4672a8510546b527e84df68876952b6965e146d816f97a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: htmleditor.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/htmleditor.directive.js
MD5: 2f49b8fc8138b308ed5d29c727b9d91c
SHA1: 78623d479efb4b319887777bdb5a4aa157d366bf
SHA256:fbc2a6c4c41ca012bd8f0aca7b941ceba3deb4f1d1f7c737d6daf92c2682e5c2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: htmleditorFactory.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/htmleditorFactory.service.js
MD5: ae7cf9f1949727b0b0abbe02d00322a3
SHA1: 8f6ca76d2a1d16c23d015e5fc99c0b5eba633ca0
SHA256:ada0a0081829c6575f5107ad1f2b857976454e420b33fb4e11caa971d23243b9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: htmleditorModel.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/htmleditorModel.service.js
MD5: 5065e5c03040fe00e77e7c35c9491459
SHA1: a07cd621341d26b6a8af98193dad1b028e518a16
SHA256:e4eb54f0aa3b0f5e3b015668ac05a9410b2fe4e2af0f796f3b9a9c1dc68de3e1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: icons.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/lib/customhugerte/icons/inet/icons.js
MD5: 81ce9691eda2df21f0904f09079b80e7
SHA1: b4a46ece9a2ab75c6aa0753ca006bc8b01d0169d
SHA256:870a4c211fd913aaee81fddc05c555949806ad233f9bdd1e5151b3b20a370fbc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: indexed-db.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/indexed-db.js
MD5: 8e18eb72cdab27b9f50d8be736fb5d3a
SHA1: 9a0e5e9098ca6fb8c1ff37a52cd41493b9c5b765
SHA256:8a7b578a09e75c8abf3b5c7796a3a9fdd812f0e1fe1b9cb2dde13c8ca4dec439
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: initUsernameField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/template/js/initUsernameField.directive.js
MD5: f3f6879a5d27234809f195e8361367fb
SHA1: 24d20461bd9e38654b9feb17b07291ac539c186b
SHA256:ce03423bc27bf8ae5f2a0ee43236549dedb25ae612839b3e645bc11849b5113f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: introduction.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/introduction.js
MD5: 89901332f1495e0cd0ee5b86914cedb1
SHA1: 35a849463bb5de9d8fc94de631c5641743d37abf
SHA256:afee3a22ebd23a8eac80d546a023e642c33409bc80ed5340e4372fc91cc30360
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: jquery.fileupload.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/jquery.fileupload.js
MD5: 240236292f36eca6c17aeac05fd73d61
SHA1: fac06f570617460bbc6f377136ee040bebad8828
SHA256:16d6dd6c899f13098e81e50b8f75ef74df0da97ed95cd2759933a13d53dc876b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: keyservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/keyservice.service.js
MD5: 727389b3179d690a641cface06314aba
SHA1: 5d3a862aea87e3c8614cefdef4cfda9ebf521b73
SHA256:a742b2d483cff1e82b6f1f2b09da02440addd6f44b2c6ba276f297c4a1c9cded
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-attribute.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/kytos-attribute.js
MD5: b316e4d0abe73690ed98456d76ae06fa
SHA1: 28e3b9464a101831d730e07b2d4d8756a0084f38
SHA256:cbaa2255f94654bbb15abd4d9019be925e1101b61625d807a942c6db7c6cd345
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-data.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-data.js
MD5: 9cd939b4d214a138e1f6912d8ff4a625
SHA1: 3ce6b8657f6c40ef854f538bb8dcaae5b213ff34
SHA256:9a1f40e1dd80682da2c5444d0e9d39f5bf5aba82768a35df3d8d36a8f27eb1ef
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-draggable-listitem.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-draggable-listitem.js
MD5: a75a0af0bc928e958f927fd6a0b54848
SHA1: 597d004880e28553c8f46912b320d935b17efcf6
SHA256:2e97d801e932e8190d02ca979fbae6513a05dd5ee38bdbae34477d4477922ef5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-dropdown.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/kytos-dropdown.js
MD5: fc087fd237309cce6af4c2018af734d7
SHA1: d8750b28da1e4b74b8283b898bd360e5b3ecbcc3
SHA256:a9b55b21c49a48b94a087bd5fbf42f99189e42a7beb07f4e656afa4b66e9a320
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-element.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/kytos-element.js
MD5: dcd2cb6e2f1f2a64b198c0d46c210144
SHA1: abf7062312f615c2d671cef520bcfb55c4ed1e34
SHA256:7f03a6a4cf815363f8a07d16ecc6fd290a6c21a4578c4337f2f695c9449aafe2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-i18n-placeholder.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-i18n-placeholder.js
MD5: 1ecbf85231e6df5bff93793f9da0dbf9
SHA1: 75494133b8f634d822291571901a5109829747bd
SHA256:85ca7c13eb0480386706977d017135d56243acec9744a44caf2bd714cedecbed
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-i18n-title.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-i18n-title.js
MD5: 4f13ffa1afc6de1e18753b8ff571eb11
SHA1: f2800872e2e0e70ffe69f2ceaec407dc2dc15102
SHA256:ca4a0fe0850986808fb897b6e2e408010bd743cb6f98a49eeb137f42d8b40ecc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-i18n.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-i18n.js
MD5: eef1960599366e9ff7c002476339991e
SHA1: 098c48087ecf44e0084693623b2bbbfb9609c115
SHA256:a320b34e638aafd53882cf205a1b811e73157023e017ef40744c3e5b640a409f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-on.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-on.js
MD5: 364260b48161e2fdf989c4f88540ddbe
SHA1: aa0924659733d3b10152b3d3ef9bb6173294b06a
SHA256:4bebd05c257fd988b34b94c75e5c90705eccc9021616c6b65a0b7d667fa67966
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-popover.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/kytos-popover.js
MD5: 8c348f49f8cec1ae88c9234673fecefd
SHA1: 9c481b02c8e3046a47afa090857a41f2a76a5e00
SHA256:1ecf2fb7edeb687b2dc1f7d258072119b5841657891044986b4f24fb69d34143
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-repeat.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/kytos-repeat.js
MD5: 941373d2347b53b9ccfd523581e5458b
SHA1: 3a6cc55704f1aca5b7c24b7fb920e1b7e9f479d1
SHA256:2502c60afa9ca7e4c6634e014326acd7d3d73dd4b8b308a95df655c861dd9319
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos-src.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/attributes/kytos-src.js
MD5: 09f25c077e3e3974fcf58c68fcca7200
SHA1: 609da5e117dce86a60ee4f330ca7ff224f876d84
SHA256:3d4758eb630910a186ecea7d5643aaa5414a504dd2a907bb844d4b9c13d39851
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: kytos.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/kytos.js
MD5: e66d46766a2db4cdb2d0cc59b5fa76c0
SHA1: a5068f4162e7252d78e66238fe220ee2ba58fe3a
SHA256:2ba2d0c8e3972158adec5d74212800741bc618d16e16f70b116d6c428f7e67b6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: localfilesystem.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/localfilesystem.service.js
MD5: 277d95afddcd590e0d141b2d577b5e62
SHA1: 20bcb984e60bdb0a2939939f52951e728a4f0af7
SHA256:07ed33c8a8d0f7931367e1c0138049de8105adefde3fa138dd50e4c7a31f8aae
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: locationservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/locationservice.service.js
MD5: c0890f9480e32f588ef16059978b3465
SHA1: 474bd66838e82ca447f1fc2a0b815b8d10c5f167
SHA256:325c4dce0b6720b72fce30d9fb0c5ba947a92854690d3a54537b084e3084abbb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: modal.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/modal.directive.js
MD5: 8b4f5159c55d2de4f772c61b5bf7dcc3
SHA1: 6d4df793d2fbad75c24f62e005eefa9ed62954cb
SHA256:2a5553a5186b68c5f299d2e1f274ba754bf9af25bcea981725d472dd762d9e42
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: modalservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/modalservice.js
MD5: 5c2c1e3b146b9ca0b16c4561205266a0
SHA1: bc64cb5a2277ed68bcf3cfc0cabeaaf8e7da3333
SHA256:83346014835ae5323f1cc77b3e096cb95d21bab053c23654763b553fd5379050
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: modalservice.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/modalservice.service.js
MD5: 1a551ec66dae8370a3470b0f9fd72467
SHA1: cc24ed601df4528c7ab569c8a67b0782f224c695
SHA256:c88cfc6dda9f889ded182a3dc4cba434998762b267c2c984471896ec26e80fa4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: moduledragdrop.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/moduledragdrop.js
MD5: 3958a1734972672ba1c124b1ed886668
SHA1: 4eb0ba0abaf32269baf7023edcaf12cc623783d3
SHA256:10d5980e1ab5d292009b20fd37d4d53367a0f76a55bd04b545074ece66d20a25
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: navtabsoverflow.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/navtabsoverflow.directive.js
MD5: 0ce7f7b7b6a5a148404b16e1962caf60
SHA1: 8ef17d2fe2fe1832fa5c49d6d65b6ef5fb1b7bdf
SHA256:b3557a1661a5cb1508bb1654d46bf5938bacaad8b4dcce03cf86d729793bd47e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ng-hugerte.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/lib/nghugerte/ng-hugerte.js
MD5: b994339b9032705280ae6a845b0af9f5
SHA1: b13ea6953e4629ac05bcb063cde294d00ad305d5
SHA256:8ff123b40a107d1f58cc63f7d5fe8921bd57a16dcba4dc7337f87b9a5cfa675a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ng-i18n.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/ng-i18n.js
MD5: f70ed5b4b0d12a1df931521a5bfd4d55
SHA1: 2f141a8d67bb4381b248e0292c2b566eb17d6ea8
SHA256:f8c9dd393e16101f533ed78c9c7d84eb60aeadd228f3573950b0930221c6425f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: number-util.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/number-util.js
MD5: 05d0f35b5c89efea5c77f9775cd6bedc
SHA1: 5f3fee5a2e389e76bb0d161c9d01b2d1aff9d5d2
SHA256:e14c43e61d7a5c8afb3c41ac057e3c49b408ef29b84bb1d4a00e43554bb51af6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: numberUtil.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/numberUtil.js
MD5: fc50f41d150aa956d3405cf5538d0ef8
SHA1: 36dd5feae806c1dff8a67fd8ae4c4b4ac8d590b1
SHA256:0a6ba6dc2719ab3741995db471ebc7e94594f837227eaad277bec79785ff9eb5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: numberValidatorUtil.factory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/numberValidatorUtil.factory.js
MD5: 5cfcc7ddeb5ee5abe9b657cb4c4aad1b
SHA1: 3e1befb49a7e3de749bbf7c11db74fad428ac1a0
SHA256:b098b08a665832d5ec3cc30a813f3ac471cc62b9f9362125b8fbc879d5d6be66
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ocLazyLoad.jsloader.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/ocLazyLoad.jsloader.js
MD5: 6efc2b278388ff3b8fd01d214f68de95
SHA1: 1d366d752be481f2502ad6e928bf443dc1bbc11e
SHA256:7c22d04e3e40f316fe62e2df4c73ffe9ca1fc552117386466972ad8a524b4154
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ocLazyLoad.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/ocLazyLoad.min.js
MD5: f2d4908265b909369078aed0cfafffa3
SHA1: 2d19edef03246ca520c6b3d658e75fad0d791695
SHA256:a5f7c8f4292aba0f63174bbb86fef9e919d97ed72f80857e83065c66ddbcb5a4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: pageablenavbaractiondropdown.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/template/js/pageablenavbaractiondropdown.directive.js
MD5: 565f00db04cd686810eba88334ccb7ef
SHA1: fc89397e87e0efb5da1dfbcf3d1f17261ddda0bc
SHA256:a3e39ab34d61e335c68b31db9411d85869b5edabffbd58cf13cd8bd89ef36c66
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: paged.filter.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/paged.filter.js
MD5: 620885e608d87c0af2184057fa716019
SHA1: 99aab6b764bd796a4fad0b23da057c07f0a173bd
SHA256:7838a62ddb112a36d3f6b3ca85606aa02bc913e5551e40a1d37a2a7411f67c88
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: pagination.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/pagination.directive.js
MD5: 9072dd128b777cbe8c9a3f5cff6d1ffc
SHA1: 9aff2deccd8bd06b84530f2759b5d3708496680c
SHA256:fe2e2a1a9bd791563352ef8b3350fc0bde4b50ae191a675e4a0fb5d592389778
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: piechart.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/piechart.directive.js
MD5: 57b1a6b4c82b90c7ae6728361bfd83aa
SHA1: c4010db7bf32f2263f721e7d0642b0e4e99b7e2c
SHA256:514ec005ce503ed102e409c830b71a04afda4dec41d04cf23e4a80f6e1def184
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: popover.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/popover.js
MD5: 24e950e89aace08f1aaa17fd06bb396c
SHA1: 1b794fe5f9c1c3015159425162f6b3b167ff1665
SHA256:4deeedf673d7fc514627d7ebca5d4595a76c7d11d9cf3bdeb720dd6f663666c6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: pwa-service-worker.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/pwa/pwa-service-worker.js
MD5: d2e662ef7530abd8ef869c584ad5c5f7
SHA1: c2ef8f57422ceea31483f489c0bb723936e7d1ca
SHA256:750f5043e378d170b3e0ae4dbe038d3dbf21caf110c84dd7860ee3f95164bce7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: pwa.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/pwa/pwa.js
MD5: 44a88e4fce9f2b6b1393ba64f8f847f7
SHA1: d3e5dc3af271d477796e38fa3f330835c636c0d4
SHA256:8c9eb4c33114482d7612e8f3438fe291a9f46ea88832e37ed214ce1f3bc229a2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: qrcode.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/reporterror/js/qrcode.min.js
MD5: 4b36f8e71a871112384d908a90471a76
SHA1: f103f61ed24f3dd86bbee1aecb91ad4ff0a15282
SHA256:6afbe1ebc2ba9b4bb0833f9f55c4eb80edb582903ea9611a9be49633a7aa3b09
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: rangeSlider.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/rangeSlider.directive.js
MD5: 8f0195ad048023303ca75052988a2958
SHA1: f30f14dce0300f317db5ad815d452dccf20c6726
SHA256:20efc1b10baaf76c2d287f1553ab7650017d266804f3c8859c8abbfd89e3766f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: rating.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/components/rating.directive.js
MD5: 5e99f0d2d98212c0aad7eacc5b6fdc19
SHA1: 1cc9c81d8b04f0eb92df48e4122a2ef60bdc74c3
SHA256:ef0f4a4cf7c466c825cf45ba1cd5cb844ed3679191f76ff0e10efab0dc0b521d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: resizableDivider.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/resizableDivider.js
MD5: 92155894052072c1b3585f3f378ed64c
SHA1: 284e63d9a8d92f3227dabbba220ce81b406fd5f7
SHA256:46db0e3c06217214be457419fa2e4a0df6dfbfa6424e163b2c9315162a9711a7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: scrollabledropdownmenu.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/scrollabledropdownmenu.directive.js
MD5: 6ccf4fe00949b9ba0161679c557720b7
SHA1: ded14570028ed526c18dba9174881e0dd4c60ae3
SHA256:aea1486dfd6055925eaceaed65bbe26260cb5a9fa6bf17acfcb4655308e34d1c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: search-input.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/search/search-input.js
MD5: 098480be160aedabd43a440be2ee38ad
SHA1: 053ff493232637ac1bbdb402953933f384a19d98
SHA256:e0056c239e493ca8652f6f77f92acc6b6d1aa621fbcba513ad118410e98f654e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: search-panel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/search-panel.js
MD5: 6911bdd8585fedc18ef1391551b7ba45
SHA1: d7c67a0c55155c887d38c4f1994a65807178d449
SHA256:162485e0b44e7f1456df024c17b0c465b6cc77b8ebbe6af9c59742b3d8d49940
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: selectInput.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/selectInput.directive.js
MD5: a5571ab4f2fdfe62686cf8b1eaa6ae6e
SHA1: a35ba49d4c09cba89b726326ea56ccb6d4f8796c
SHA256:6f813a891ac8eee591a2b57073f534e9b611c2c6b3c73b80e57bc71abb00557f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: settings-ui-search.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/settings-ui-search.js
MD5: ae95b86fbc2103b650093dca6cbc8c65
SHA1: 454531a07199b99bb35571d159d6982b3f21ed0f
SHA256:3c49fe2960ac460ff92ce778c70e481feab5c931c1159571646fe832ad9b34b0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: settings-ui.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/settings-ui.js
MD5: ffff0524a271161a40a189ef21721832
SHA1: bb4df4e783021d2916f58fcf976e1fa981369f87
SHA256:93e526593e4f04c84d90fc5f1d016b033cdae8ca96edc6bb3259520a01ea6dc9
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: shadowLogger.factory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/shadowLogger.factory.js
MD5: fa91436385b8994b55a7d310d63aae1b
SHA1: 6dcf22bc7bc7561e394ab64f4cd68935378b77cb
SHA256:99d32693c3484880d4e331ee348efbf9a6c37f657a63045a1f50ef3e8dd3d60c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: sidenavigation.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/sidenavigation.js
MD5: 66033ba764d884e192b1c7c358d720cd
SHA1: 0ff133e2f528d17251cb0c3afe505c0296867a78
SHA256:9aa9ff3d296d25898a01095a5a1f0b2257a84dcf442a99890bd6bd6587c32127
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: takeoutDataController.controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/takeout/js/takeoutDataController.controller.js
MD5: 82d1cec699a839f96167893738956807
SHA1: b0c88a87252c6c7c558b366e8f8c8b85179cd354
SHA256:48b31ddfab8b1f4607a020ba89e0cc44d41fa7d29e440224d794f494186a70d6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: takeoutDataFactory.factory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/takeout/js/takeoutDataFactory.factory.js
MD5: 4c2e4791571aa7c4beef1d13e162b700
SHA1: 72b5880e8daf6c9ff20aa30132fe79c7f4868ca8
SHA256:7cd1066a0db5c12af802b239d6d2b1d0afa29c5417460189ae5c22f5c6c3484e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: takeoutDataModel.service.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/takeout/js/takeoutDataModel.service.js
MD5: 6bcf8a37b4157e9c59412040d832b2e9
SHA1: 12b1e7fb37e1533e850a261eb24e5260e42368f8
SHA256:9a256e7e32f5971e086b0aa0e02d74c9b128fa2b2700a957af0282d8a1387d72
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: timeInput.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/timeInput.directive.js
MD5: ba7319d83a3bcc33e0019d36fdfef0d9
SHA1: 019c707edf3c03914faea76cc116043f51a55ca2
SHA256:ae9ff67469f81911d87d69f7e89d7651b2517673b0a1538f04fb64076f5d0c70
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: timeInputContainer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/timeInputContainer.directive.js
MD5: fbc7a8c9f4e3a3cc38d7659d83a6c29e
SHA1: 6b62e43062fdea0d9a6d7dc537e8be85787990a0
SHA256:13eb8eba0cfd94da346f8cd131a4f90c98261fd83473d80c6c4b98529dcb7e1c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: timeMeridiemContainer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/timeMeridiemContainer.directive.js
MD5: e1458f3e6ea63204589509e5237f5c31
SHA1: 0a3f9057c78f591a1bb4086e1910af248290e689
SHA256:b9663e93c6051a50803d0425bf1da08bb6079b7eaedfbbb88f073880cd833088
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: toastservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/services/toastservice.js
MD5: c1e6d55ffb1832de666a82a5940d3481
SHA1: bdcef38fc0117a5abc6e2e81aaed372ce6b2a677
SHA256:ebb72d1b0d2b92dafd57933bbf927401edafc083883983dbf984f175a3fbd023
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: translate.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/translate.js
MD5: 061e99802cbbcc1f551b74ad18d8f5e5
SHA1: 941904c2d0237f7941cd16a088d3cf943a8628d7
SHA256:eecc08ab9f22b266c4c1ca774958609372959797bcbc2ef9be0d68fbeac88ced
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-checkbox.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-checkbox.js
MD5: 7a452f508c13b4ee8471675e16073f46
SHA1: 010958a3f2ad052e6f0be4dc6d6e0cfc851bfa8a
SHA256:a2d2c3e79d33a16c3a9706f81f8a78962bf36b789c1d4b773f13bac16d53f824
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-chooser-color.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-chooser-color.js
MD5: d3304eb7504d61dbfb0292358b17e043
SHA1: 33c5194e987fba381eaa15a3d2e7d32a34c5d6ff
SHA256:021b196cdc3ee25c10b11c7b859ccc6822ec36c986ef7c3a35e6d842f651f8b4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-chooser-file.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-chooser-file.js
MD5: c91f3875e0258f351960764aef9e8031
SHA1: 6f95a34158c34b28387c3a1c9da55a68f5c9e810
SHA256:366270e3764fcd1a146296530ccabfe3920a5a60caf248ddd3381b3c1992c43a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-group.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-group.js
MD5: ec02a3c46d5bca390d0bdb1cfb97928e
SHA1: 2f868299f06990eef6f97e4936492b7c599af33d
SHA256:43a5181441cdc72318a4e32c8b65b41df6e4cff4a5eeda0e1b55227d9c9d4f60
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-multiline.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-multiline.js
MD5: 7e4ee6704cb4ac8fcd86c7b9c706fdec
SHA1: bdd14f8f1a09fa4a143b0d62ae1a0b96ff4bf80e
SHA256:f11f704fce177a76988f84ba90c5ac2541a6ef3a975749f7d14644627074037d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-number-fixed.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-number-fixed.js
MD5: 060fb11b6347bf83647c5759d263b02b
SHA1: e619f0f7ec0c840a07a6c0ce9ae09790090651cd
SHA256:3e44507e4bdce3449feb8419eccffd612a59a107ddfddffc1ac20b184472f26d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-number-float.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-number-float.js
MD5: 8f2c86f4d7d4290c2676ec199be23617
SHA1: 55a03258d2b0d0ad0abc19e30b30f5e58ce08e92
SHA256:156d6e7bbedbbd4ba1c0bbe5e20da53300e92710cddd37b6e309dff38beb139e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-password.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-password.js
MD5: ad91a95258914de2102067d9ced743d4
SHA1: f2b87a068b74229764561d3d79a4680deb91396b
SHA256:efe868282707158480f36879da25d44d40075b9c968ed5bfffb5d7dbaaf04e89
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-search.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-search.js
MD5: ebc03148fb564c80bb9e54856361c9a9
SHA1: e1f96614e8f51f6521db36102527336681739a82
SHA256:a15d49a0efd3c307dbdae15a1280cec83310aad26f1238b648dd89b1915626fb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-text.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-text.js
MD5: 91e3d37564c843ad38d2f0d6c8abecc1
SHA1: 3d2c65c121ddc2141dc13bf34ee02f50bce47e5d
SHA256:e0d1f7a167d81a1d1e7b8c829fc7df342e1177c0475cbaa1ca99c9fe47456d8d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-input-unit.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-input-unit.js
MD5: 402351045833df47a0c08c612685d0b2
SHA1: 4f808ee68dd70e0d0388b7ad57b42ab09a259f65
SHA256:cbef23fe0d828957d788e38407cd8f7c489ad73354e0f021b088663e0a36127d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-label.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-label.js
MD5: 26e292fbb5d3c87d5c314504a0fb0e56
SHA1: 641f118b4ff856a5300a6d20627bb518901a714c
SHA256:11db374eae7ff2d8975cfd9eb32cb5227be4e8af35ac3932f385a789fa862fff
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-link.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-link.js
MD5: 6ff3511d10020a8db068bbd946db2543
SHA1: 7a605e2f755ed92b794892f917e672c129dc4431
SHA256:b4acabb5d6f690cc492b525ffee0391df5297a0fbecaf029db08b542213dde56
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-multi-property.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-multi-property.js
MD5: d2a8671a07f908fdee85b885a8194374
SHA1: 19c14e8f885af5cae7a268c4cfd6b2897bcbe9f9
SHA256:e983ea3c288bfe07d0f377ee2747bca012b01a19f449514a97d5168e30ac91f3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-property.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-property.js
MD5: bf03c87292120a03c4ba801e6f9aa4cd
SHA1: 512476332ff73997b41a56e6104433ad82f48747
SHA256:f6126adffe7eb1b60282e161b1598488958422ccb6326c8773b26e8478b7514f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-radio-button.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-radio-button.js
MD5: edc476289a12735f271ba1d50f846536
SHA1: 16560d85f89f8ea23529e05192e8b91112802073
SHA256:4643ce0f15cb8ce1deb7a2ac4d0f36ab10de70c639559b3b81adcce368cec81a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-section.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-section.js
MD5: 2df0c0acad3fbb332450956fabc7c4c7
SHA1: 9ea8b3117f6533fd3917c08669ed896560df041e
SHA256:bbf8170e8e33f502fb2979771e8534b71d0e16b088f29c226a11222213faa010
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-select-edit.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-select-edit.js
MD5: 12abe1a1ee37fd3820857990111c1995
SHA1: 8401589071d4d5616fcd2df5e31bde58d2c34adc
SHA256:53509ca221383c059d5a0b75b8b20a0e8e3b904235108db9e69da2b2cee79f6c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-select-filtered.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-select-filtered.js
MD5: d4524658076aeaf86140df1b19f8ecbd
SHA1: 0bffe996e07c731c52421dd11e97755f07cd22f5
SHA256:b158e97a9c401c79d00ef6c825a13e3c0d69c7a20d2e236208b48d4267ffaef6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-select-options.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-select-options.js
MD5: 096af83c910cbe2bf12963c11d71a9b4
SHA1: 02b69897cf88dc37383e12f7334114b1c4a15033
SHA256:c745075492b26fbbac7e12479ab36a9744042f69a598131a3b8099af3d2f99d2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: ui-slider.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/kytos/components/settingsui/ui-slider.js
MD5: 7e96cde9ca1663b2f957d43e3e2416e2
SHA1: 157706b9e7c2e5568c1e08d6619296712c1fb524
SHA256:6c24994677b4fde59b8e202b9518468ec7b1b59c975bcf86084848d931067425
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: unitFixNumber.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/unitFixNumber.directive.js
MD5: 29d24835a3a3f09d56371f64a9e5501d
SHA1: 74508076d24cd85f342390ee1809e2bb70f48839
SHA256:6a20d4eca5c69740c0fa2f99c209aed92ffa49c48848e3ff63ab6fc9b2f6ac32
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: unitFloatNumber.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/number/unitFloatNumber.directive.js
MD5: 1d3c2d9b2853e77c53b7f755e4f82bc0
SHA1: 56134dad87141744f8fee3574ebde43a96484ce5
SHA256:dde76e45fa7be7de9e04b3eb5a33954d8c2470636fa945458c08031b593b7492
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: userservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/userdetails/userservice.js
MD5: 2dd0b8375265a6ed68641819428de40a
SHA1: 6dd8650e16e461e04b2261d6d8e3c0992e451e5d
SHA256:3221cad085226391898e3d6fc0a9bdd431e46fe035d13029e89cbc497ecf6a28
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: usersorgroupsselection.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/usersorgroupsselection/usersorgroupsselection.js
MD5: 04a58b219c040f41230ae126a006c59e
SHA1: 67e9ab78d477b7cd7c5cbdc28d47673dd16919c9
SHA256:76d9a0d819262d078eac80f148b41121d203fdb7c6292bd5ced5d7626bf9816b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: usestrict.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/usestrict.js
MD5: 8e742d11d6b24c401e35f3b516726584
SHA1: 89b72153bd7e6390415ba25b9b5fbe750e6e16d5
SHA256:8e8cc72e61ff6f6c0c945a976756d112732c499cd64fc5b207bb213fc84a1e40
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: websitedownload.renderer.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/modules/website/js/websitedownload.renderer.js
MD5: 997a09bf4e3740f123d6933770b57ed1
SHA1: d59541fedeba1aa388dc41757bccde3f35324d1a
SHA256:53a3d1d2454b0730a885b126c853b9ee7a53ff1e01266fc2aae4b758fa1dd7a3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: websocketdataservice.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/websocketdataservice.js
MD5: 07f76c0eefd17b8aa728237315e93c2e
SHA1: bfcaad46fcfea2e794f774c2242980697e9515c3
SHA256:e686d40da6bb55c6be775f10f9cca223d91fdf5e532655d5107aa2451c0994b4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: websocketkeepaliveworker.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/websocketkeepaliveworker.js
MD5: b378595229f68cdd9acc7775a85e3746
SHA1: 5eb59a40044f9cfb861f3c39cf4969cb7e969323
SHA256:d695e751ea4e77b998aefab636299872246f04af2b189623dde151cce2fca67d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: remotegui.jar: windowdatarestore.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/remotegui.jar/com/inet/remote/gui/angular/weblib/inet/js/windowdatarestore.js
MD5: 574aeff88e7d16bdfa230828b48f23fc
SHA1: 8befdf89f00605b0c8481f2dfccbf6feca9c07be
SHA256:9e569b372029c31a553329de89c192020c9cb8dbe9664ddb1b9c9ee4507e3a18
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

remotegui.zip: twemoji.jar

License:

MIT

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/twemoji.jar
MD5: af9b535ef495075dfb0a7d5bec95eee6
SHA1: 0a559adee289b6b855ad1294b17dd71d9f3d21eb
SHA256:9ce4f61ef563851b37c3918c54a876a865d2f66fda5f80dd2bfecebb2d7e386f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	twemoji	High
Vendor	Manifest	url	https://github.com/twitter/twemoji/blob/master/LICENSE	Low
Vendor	pom	artifactid	twemoji-null	Low
Vendor	pom	groupid	lib	Highest
Vendor	pom	url	twitter/twemoji/blob/master/LICENSE	Highest
Product	file	name	twemoji	High
Product	Manifest	url	https://github.com/twitter/twemoji/blob/master/LICENSE	Low
Product	pom	artifactid	twemoji-null	Highest
Product	pom	groupid	lib	Highest
Product	pom	url	twitter/twemoji/blob/master/LICENSE	High
Version	pom	version	1.0	Highest

Identifiers

- pkg:maven/lib/twemoji-null@1.0 (*Confidence*:High)

security.zip: security.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/security.zip/security.jar
MD5: 87bb5eb1ea35fd79a559c638b1f972c2
SHA1: 333e8f986db35c2c81c7b4fc7c70c5c48ae42370
SHA256:b84cfc4e6907162d1e5f8d723bb0ad58ade29d98b80ba6ca1c05983b726403ea
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	security	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	security	Low
Vendor	jar	package name	server	Low
Vendor	Manifest	built-date	2026-09-28 17:40	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	security	High
Product	jar	package name	security	Highest
Product	jar	package name	security	Low
Product	jar	package name	server	Low
Product	Manifest	built-date	2026-09-28 17:40	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	security	High
Product	Manifest	specification-title	security	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

setuplauncher.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/setuplauncher.jar
MD5: 4e451ae93134440e91e6087d86bca9bd
SHA1: f18c88593fa194a5f511d05e2f0d036e5b8d1477
SHA256:7bc05d66c2a8f8509263bb9c8d383f2d7761ddd595c217b6be44285e5df98eaa
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	setuplauncher	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	setuplauncher	Low
Vendor	Manifest	built-date	2026-09-28 17:23	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	setuplauncher	High
Product	jar	package name	setuplauncher	Highest
Product	jar	package name	setuplauncher	Low
Product	Manifest	built-date	2026-09-28 17:23	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	setuplauncher	High
Product	Manifest	specification-title	setuplauncher	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

slf4j-api-2.0.18.jar

Description:

The slf4j API

License:

https://opensource.org/license/mit

File Path: /home/jenkins/.gradle/caches/modules-2/files-2.1/org.slf4j/slf4j-api/2.0.18/78a9e7a37cd6360e0b818e86341b24123d28d4df/slf4j-api-2.0.18.jar
MD5: fe2837bd49bfb76657419002fed20ca9
SHA1: 78a9e7a37cd6360e0b818e86341b24123d28d4df
SHA256:44508fd1576500688c790b190acdd16fec4f8c79a3e0b900afd70503cf055f55
Referenced In Projects/Scopes:

- CoWorkInstaller
- CoWorkInstaller:inetPlugin

Included by: pkg:maven/cowork/CoWorkInstaller@26.10

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	slf4j-api	High
Vendor	gradle	artifactid	slf4j-api	Highest
Vendor	gradle	groupid	org.slf4j	Highest
Vendor	jar	package name	slf4j	Highest
Vendor	Manifest	build-jdk-spec	21	Low
Vendor	Manifest	bundle-docurl	http://www.slf4j.org	Low
Vendor	Manifest	bundle-symbolicname	slf4j.api	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	pom	artifactid	slf4j-api	Low
Vendor	pom	groupid	org.slf4j	Highest
Vendor	pom	name	SLF4J API Module	High
Vendor	pom	parent-artifactid	slf4j-parent	Low
Vendor	pom	url	http://www.slf4j.org	Highest
Product	file	name	slf4j-api	High
Product	gradle	artifactid	slf4j-api	Highest
Product	jar	package name	slf4j	Highest
Product	Manifest	build-jdk-spec	21	Low

Product	Manifest	bundle-docurl	http://www.slf4j.org	Low
Product	Manifest	Bundle-Name	SLF4J API Module	Medium
Product	Manifest	bundle-symbolicname	slf4j.api	Medium
Product	Manifest	Implementation-Title	slf4j-api	High
Product	Manifest	multi-release	true	Low
Product	pom	artifactid	slf4j-api	Highest
Product	pom	groupid	org.slf4j	Highest
Product	pom	name	SLF4J API Module	High
Product	pom	parent-artifactid	slf4j-parent	Medium
Product	pom	url	http://www.slf4j.org	Medium
Version	file	version	2.0.18	High
Version	gradle	version	2.0.18	Highest
Version	Manifest	Bundle-Version	2.0.18	High
Version	Manifest	Implementation-Version	2.0.18	High
Version	pom	version	2.0.18	Highest

Related Dependencies

- slf4j-api.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/core/slf4j-api.jar
  - MD5: fe2837bd49bfb76657419002fed20ca9
  - SHA1: 78a9e7a37cd6360e0b818e86341b24123d28d4df
  - SHA256: 44508fd1576500688c790b190acdd16fec4f8c79a3e0b900afd70503cf055f55

Identifiers

- pkg:maven/org.slf4j/slf4j-api@2.0.18 (*Confidence*:High)

taskplanner.coworkmessage.zip: taskplanner.coworkmessage.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.coworkmessage.zip/taskplanner.coworkmessage.jar
MD5: 37501d6aabb1971be98eed58039e7d40
SHA1: 452cfa1fe23e19459c13b6462ec2bb8cf7801dad
SHA256:9c07f65dc85c8b7fba91d47bec731e14dd97d8df87b17724f79eb90b0702188c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	taskplanner.coworkmessage	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	plugin	Low
Vendor	jar	package name	taskplanner	Low
Vendor	Manifest	built-date	2026-09-28 18:05	Low
Vendor	Manifest	implementation-group	cowork	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	taskplanner.coworkmessage	High
Product	jar	package name	cowork	Highest
Product	jar	package name	cowork	Low
Product	jar	package name	plugin	Low
Product	jar	package name	taskplanner	Highest
Product	jar	package name	taskplanner	Low
Product	Manifest	built-date	2026-09-28 18:05	Low
Product	Manifest	implementation-group	cowork	Low
Product	Manifest	Implementation-Title	taskplanner.coworkmessage	High
Product	Manifest	specification-title	taskplanner.coworkmessage	Medium
Version	jar	package name	cowork	Highest
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

taskplanner.zip: commons-cli.jar

Description:

Apache Commons CLI provides a simple API for presenting, processing, and validating a Command Line Interface.

License:

https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/commons-cli.jar
MD5: e689f5e4947368dd0233fc28f613f561
SHA1: a461452d3e31bebf2706323f8738ec44b19c96e1
SHA256:8f7f8605d68e15bf32db61ec94eac6fdafc51b1bdbe1e0e0802b57d23f387792
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	commons-cli	High
Vendor	jar	package name	apache	Highest
Vendor	jar	package name	cli	Highest
Vendor	jar	package name	commons	Highest
Vendor	Manifest	build-jdk-spec	25	Low
Vendor	Manifest	bundle-docurl	https://commons.apache.org/proper/commons-cli/	Low
Vendor	Manifest	bundle-symbolicname	org.apache.commons.cli	Medium
Vendor	Manifest	Implementation-Vendor	The Apache Software Foundation	High
Vendor	Manifest	Implementation-Vendor-Id	org.apache	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	Manifest	specification-vendor	The Apache Software Foundation	Low
Vendor	pom	artifactid	commons-cli	Low
Vendor	pom	developer email	bob@werken.com	Low
Vendor	pom	developer email	chtompki@apache.org	Low
Vendor	pom	developer email	ebourg@apache.org	Low
Vendor	pom	developer email	ggregory at apache.org	Low
Vendor	pom	developer email	jbjk@mac.com	Low
Vendor	pom	developer email	jstrachan@apache.org	Low
Vendor	pom	developer email	roxspring@imapmail.org	Low

Vendor	pom	developer email	tn@apache.org	Low
Vendor	pom	developer id	bob	Medium
Vendor	pom	developer id	chtompki	Medium
Vendor	pom	developer id	ebourg	Medium
Vendor	pom	developer id	ggregory	Medium
Vendor	pom	developer id	jkeyes	Medium
Vendor	pom	developer id	jstrachan	Medium
Vendor	pom	developer id	roxspring	Medium
Vendor	pom	developer id	tn	Medium
Vendor	pom	developer name	Bob McWhirter	Medium
Vendor	pom	developer name	Emmanuel Bourg	Medium
Vendor	pom	developer name	Gary Gregory	Medium
Vendor	pom	developer name	James Strachan	Medium
Vendor	pom	developer name	John Keyes	Medium
Vendor	pom	developer name	Rob Oxspring	Medium
Vendor	pom	developer name	Rob Tompkins	Medium
Vendor	pom	developer name	Thomas Neidhart	Medium
Vendor	pom	developer org	Ariane Software	Medium
Vendor	pom	developer org	Indigo Stone	Medium
Vendor	pom	developer org	integral Source	Medium
Vendor	pom	developer org	SpiritSoft, Inc.	Medium
Vendor	pom	developer org	The Apache Software Foundation	Medium
Vendor	pom	developer org	Werken	Medium
Vendor	pom	developer org URL	https://www.apache.org/	Medium
Vendor	pom	groupid	commons-cli	Highest
Vendor	pom	name	Apache Commons CLI	High
Vendor	pom	parent-artifactid	commons-parent	Low
Vendor	pom	parent-groupid	org.apache.commons	Medium
Vendor	pom	url	https://commons.apache.org/proper/commons-cli/	Highest
Product	file	name	commons-cli	High
Product	jar	package name	apache	Highest
Product	jar	package name	cli	Highest
Product	jar	package name	commons	Highest
Product	Manifest	build-jdk-spec	25	Low

Product	Manifest	bundle-docurl	https://commons.apache.org/proper/commons-cli/	Low
Product	Manifest	Bundle-Name	Apache Commons CLI	Medium
Product	Manifest	bundle-symbolicname	org.apache.commons.cli	Medium
Product	Manifest	Implementation-Title	Apache Commons CLI	High
Product	Manifest	multi-release	true	Low
Product	Manifest	specification-title	Apache Commons CLI	Medium
Product	pom	artifactid	commons-cli	Highest
Product	pom	developer email	bob@werken.com	Low
Product	pom	developer email	chtompki@apache.org	Low
Product	pom	developer email	ebourg@apache.org	Low
Product	pom	developer email	ggregory at apache.org	Low
Product	pom	developer email	jbjk@mac.com	Low
Product	pom	developer email	jstrachan@apache.org	Low
Product	pom	developer email	roxspring@imapmail.org	Low
Product	pom	developer email	tn@apache.org	Low
Product	pom	developer id	bob	Low
Product	pom	developer id	chtompki	Low
Product	pom	developer id	ebourg	Low
Product	pom	developer id	ggregory	Low
Product	pom	developer id	jkeyes	Low
Product	pom	developer id	jstrachan	Low
Product	pom	developer id	roxspring	Low
Product	pom	developer id	tn	Low
Product	pom	developer name	Bob McWhirter	Low
Product	pom	developer name	Emmanuel Bourg	Low
Product	pom	developer name	Gary Gregory	Low
Product	pom	developer name	James Strachan	Low
Product	pom	developer name	John Keyes	Low
Product	pom	developer name	Rob Oxspring	Low
Product	pom	developer name	Rob Tompkins	Low
Product	pom	developer name	Thomas Neidhart	Low
Product	pom	developer org	Ariane Software	Low
Product	pom	developer org	Indigo Stone	Low
Product	pom	developer org	integral Source	Low

Product	pom	developer org	SpiritSoft, Inc.	Low
Product	pom	developer org	The Apache Software Foundation	Low
Product	pom	developer org	Werken	Low
Product	pom	developer org URL	https://www.apache.org/	Low
Product	pom	groupid	commons-cli	Highest
Product	pom	name	Apache Commons CLI	High
Product	pom	parent-artifactid	commons-parent	Medium
Product	pom	parent-groupid	org.apache.commons	Medium
Product	pom	url	https://commons.apache.org/proper/commons-cli/	Medium
Version	Manifest	Bundle-Version	1.11.0	High
Version	Manifest	Implementation-Version	1.11.0	High
Version	pom	parent-version	1.11.0	Low
Version	pom	version	1.11.0	Highest

Identifiers

- pkg:maven/commons-cli/commons-cli@1.11.0 (*Confidence*:High)

taskplanner.zip: cron-utils.jar

Description:

A Java library to parse, migrate and validate crons as well as describe them in human readable language

License:

Apache 2.0: http://www.apache.org/licenses/LICENSE-2.0.html

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/cron-utils.jar
MD5: 4c27537eecc6fa37ed5740b5383643c8
SHA1: 5d3738bc7a2eaa45a94a76c6e87af54a95414637
SHA256:02af0e8b2fe93c9fa6eecf97b53b39faae14c5b996356edb132e9fe620013744
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Vendor	file	name	cron-utils	High
Vendor	jar	package name	cron	Highest
Vendor	jar	package name	cronutils	Highest
Vendor	jar	package name	utils	Highest
Vendor	Manifest	automatic-module-name	com.cronutils	Medium
Vendor	Manifest	build-jdk-spec	1.8	Low
Vendor	Manifest	bundle-symbolicname	com.cronutils.cron-utils	Medium
Vendor	pom	artifactid	cron-utils	Low
Vendor	pom	developer id	jmrozanec	Medium
Vendor	pom	groupid	com.cronutils	Highest
Vendor	pom	name	cron-utils	High
Vendor	pom	url	http://cron-parser.com/	Highest
Product	file	name	cron-utils	High
Product	jar	package name	cron	Highest
Product	jar	package name	cronutils	Highest
Product	jar	package name	utils	Highest
Product	Manifest	automatic-module-name	com.cronutils	Medium
Product	Manifest	build-jdk-spec	1.8	Low
Product	Manifest	Bundle-Name	cron-utils	Medium
Product	Manifest	bundle-symbolicname	com.cronutils.cron-utils	Medium
Product	pom	artifactid	cron-utils	Highest
Product	pom	developer id	jmrozanec	Low
Product	pom	groupid	com.cronutils	Highest
Product	pom	name	cron-utils	High
Product	pom	url	http://cron-parser.com/	Medium
Version	Manifest	Bundle-Version	9.2.1	High
Version	pom	version	9.2.1	Highest

Identifiers

- pkg:maven/com.cronutils/cron-utils@9.2.1 (*Confidence*:High)
- cpe:2.3:a:cron-utils_project:cron-utils:9.2.1:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:utils_project:utils:9.2.1:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

taskplanner.zip: guava.jar

Description:

Guava is a suite of core and expanded libraries that include utility classes, Google's collections, I/O classes, and much more.

License:

http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/guava.jar
MD5: d9fbf39a41a5bab891348f07668e18c5
SHA1: 8699de25f2f979108d6c1b804a7ba38cda1116bc
SHA256:1e301f0c52ac248b0b14fdc3d12283c77252d4d6f48521d572e7d8c4c2cc4ac7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	guava	High
Vendor	jar	package name	google	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-docurl	https://github.com/google/guava/	Low
Vendor	Manifest	bundle-symbolicname	com.google.guava	Medium
Vendor	Manifest	multi-release	true	Low
Vendor	pom	artifactid	guava	Low
Vendor	pom	groupid	com.google.guava	Highest
Vendor	pom	name	Guava: Google Core Libraries for Java	High
Vendor	pom	parent-artifactid	guava-parent	Low
Vendor	pom	url	google/guava	Highest
Product	file	name	guava	High
Product	jar	package name	google	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-docurl	https://github.com/google/guava/	Low
Product	Manifest	Bundle-Name	Guava: Google Core Libraries for Java	Medium
Product	Manifest	bundle-symbolicname	com.google.guava	Medium
Product	Manifest	multi-release	true	Low

Product	pom	artifactid	guava	Highest
Product	pom	groupid	com.google.guava	Highest
Product	pom	name	Guava: Google Core Libraries for Java	High
Product	pom	parent-artifactid	guava-parent	Medium
Product	pom	url	google/guava	High
Version	pom	version	33.5.0-jre	Highest

Identifiers

- pkg:maven/com.google.guava/guava@33.5.0-jre (*Confidence*:High)
- cpe:2.3:a:google:guava:33.5.0:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

taskplanner.zip: taskplanner-javadoc.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar
MD5: cbfd371639e99cbfc1f71aa6ef877ca1
SHA1: dd29fd39c5d56d23f9ebd3a5a6a8331fce23f4dd
SHA256:dcd9a700b93690ae8aaf4b3e067933cb56aee0bdba048e4dcd400cf9999fa9f5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	taskplanner-javadoc	High
Product	file	name	taskplanner-javadoc	High

Identifiers

- **None**

taskplanner.zip: taskplanner-javadoc.jar: member-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/member-search-index.js
MD5: 614d1d59832256e8dfc383ef2a2a1914
SHA1: d01475d6e682d99e06b27faf12034b565c614857

SHA256:154f5f9e34b71c1959bd226ccf946d73d3782c27963849e80f4872a0978a8da7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner-javadoc.jar: package-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/package-search-index.js
MD5: 255e24c89b3410ec719bc3e25178f792
SHA1: 6bc183e49cd63d4cc20af2cbeca91bd9ee190f0c
SHA256:606dafa606a4f2884b54590b2a16b160220e981209dd992bc1c0f68baf1165cc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner-javadoc.jar: tag-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/tag-search-index.js
MD5: ec278f4b13380caca9964618a9dfd79f
SHA1: 1eb71a3e466628ff69b06ea2bd04d8153c919da4
SHA256:7a1f884ab397213a8d63202a55620934550f6ca917942a91fee40d375eba9e72
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner-javadoc.jar: type-search-index.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner-javadoc.jar/type-search-index.js
MD5: 754e7e321c223acc65b527238dafa89a
SHA1: b41e084651fb24741ae73588d82b596e9aad9148
SHA256:42f25303937d360bf7f3921c8d7f90919dbe53fea5c025333c9f97642ed98a55
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar
MD5: c07727ba928c6180a593e5a3560f3d99
SHA1: 8892157db5357feb1bc573ea8588a432dec1e866
SHA256:6ddb854b4d9138e8d66fe5f02c09839abae5abb1e97d5f1a0fc8057732283ddd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	taskplanner	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	server	Low
Vendor	jar	package name	taskplanner	Low
Vendor	Manifest	built-date	2026-09-28 17:03	Low

Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	taskplanner	High
Product	jar	package name	api	Low
Product	jar	package name	server	Low
Product	jar	package name	taskplanner	Highest
Product	jar	package name	taskplanner	Low
Product	Manifest	built-date	2026-09-28 17:03	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	taskplanner	High
Product	Manifest	specification-title	taskplanner	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: app.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/app.js
MD5: 22be8e86a9121096b162ff523e37842e
SHA1: cc6010fdc028f0b9c5c95def16c69e3bab116bf0
SHA256:511c001c378b9f9e28f261cafaa88892acb5a29743c50d5daf15dd869357bc0c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: boolean.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/boolean.directive.js
MD5: 908a1e9357bec6406621160e63ac58af
SHA1: 60487d9af0a54ba8c28cfa9c7a6b16b505e95925
SHA256:1c3947ab770ec265c4e6195c2042fe011a45bbdbc25233c24934fd43486f0c7e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: colorField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/colorField.directive.js
MD5: 6befac83d2b0754235fb738ada07b8db
SHA1: fa581823e83812639dd7a834b580619472492cff
SHA256:299ff7b917c507bb852d4c8f7a305e545c214806ae816b47aa9f2b37928a5154
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: controller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/controller.js
MD5: b387569fd1f675f531f0133a95bd66b5
SHA1: da502904549d1b1402d021562d0f8e0de3ea2430
SHA256:eb8a77662109d6b27001027d47d65ba0ac8401873bf26037a65e2a078598f667
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: factory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/factory.js
MD5: 0833616fa9d598778a535defc186b8a5
SHA1: aeaf34eed94c453087c31b97d76ca1c6f2036f56
SHA256:c3cae7edfe608691b9a7661fd0b5617c138993e2f9c1f9bc31449c418f5d268d
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: filechooserAddonButton.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js

/fields/filechooserAddonButton.directive.js
MD5: 1dbc17a2a4e1fc7930dda7d5d3e4630a
SHA1: 350be18d05b89c69fa3167a09822876d21a42143
SHA256:140100d27da0900d67a30dadcf9971ed9eff5c2787aa5814b930f986615c6abb
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: model.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/model.js
MD5: 64c16f108758b004347ad7a2bda6fa24
SHA1: 8764572c20ca459b4b3b0947a21d59770bf6f451
SHA256:f8635e1599cabfe239f25cd31d564e83c0fd045de00bdcc9c09783323667c722
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: numberRange.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/numberRange.directive.js
MD5: e98f0aec3fd059575c390f4488396764
SHA1: 5fb36b30f1022112f5da2a9373fa562859a8f05d
SHA256:2164d0a1c06a1750c41b3be860ade120946d0091f3f6c512241235601c3f74b6
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: numberWrapper.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/numberWrapper.directive.js
MD5: c71128c3dac942fc1d5d488562b727a0
SHA1: 51e1419abd22f7f48debceb976752bfec46e36f4
SHA256:3c3f6b8e5bcc8bf32a3cf2192a10de8472100d195cc2b08c4ff860a0dcb9bacf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: passwordTextField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/passwordTextField.directive.js
MD5: 713a6a960fdcaa473c4e4df8a795327b
SHA1: 169a814e8be8d374ef506df6ffe4c7e5a6d86649
SHA256:05fa24c6f3246de2577f8b0656e952db6e011346ec942dc8a9a27ded9de39f11
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: renderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/renderer.directive.js
MD5: 3e232b940bcd532e99c88f5b95bf60b2
SHA1: a051ce6df82ad9673fc1b23bafc3670d70bb4cac
SHA256:b930dc86802f4307b5f6d4671f27dac5bd85d5766f32567f5479ecc9077bf5a3
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleCurrencyField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleCurrencyField.directive.js
MD5: 54ae56c2f76e7b601b9e9785dc51a623
SHA1: af05845b893807b4460bc65fa189700abcb4dc82
SHA256:847d6da58f5887edac53896e6bec4dde5b293a08a8ac6e421aa2847991f3b877
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleDateTimeField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleDateTimeField.directive.js
MD5: 53d33b9956ea6ffea7cb1fef5e878961
SHA1: 2388423f76a1b38cb2e5729e57a113245e1d3f2d
SHA256:7cbb2507fe22dfec607af8d76d85317a395c3ebb98e31ec9be26e73350dbcd9f
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleFileFolderField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleFileFolderField.directive.js
MD5: 76de6683bc2d43547059d2f746b9524f
SHA1: c6ce84f2d2a89f07c4f05e95137abcdade89cec5
SHA256:7e15aca0687784f1221b8c76328af4d013a0a1573a56232d880c4b60cd3311a0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleGroup.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleGroup.directive.js
MD5: d69a3c1dd5569172999325602506517f

SHA1: 780808312f5a19e0b6726453655b1911dde585bc
SHA256:4eada3908c9db4213e058eb378f9f7f28e7e96e0ee3de2817f5d408b88176dc5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleLabel.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleLabel.directive.js
MD5: ecbe7da1cc7d51e0bd4e73e7c2fad4df
SHA1: d16a32bb34f1ff4d0f4740a06660ed72f4eca1fc
SHA256:2b533fa13f74789de6b02fb037bfd7eae3b8b6e7d0f851a66f57739f565fd453
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleLink.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleLink.directive.js
MD5: 525dc45cb1886c4808186e1094480bba
SHA1: 7198a40b645128e0495d6d04c008b31b37faf827
SHA256:7f2b60bda8c8e3938f9e8762c000606909ba0411aa784a202c93a1b2371cd82e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleSelect.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleSelect.directive.js
MD5: e54a750acec037585e380229a6b74b39
SHA1: a6323f355bb4da4cdcac24be2572fec96332bfa8
SHA256:39d6b66fe24beb027a1445157af449f17a51069e0887603b4eaf624474b5ee6c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: simpleTextField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/simpleTextField.directive.js
MD5: 998a4b2340386c5ff39fd74451642547
SHA1: b0025705125d1a18bec3624d0eb34176bb332c9d
SHA256:8a7ad2a61dbd1c78565a7626a8c100523c97984be77d431929041f19e2f24c1c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: stringTable.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/stringTable.directive.js
MD5: 2731ad8625d24769bc3f9727361b4d6f
SHA1: d0c7a2e05d815252c80a51064ffe4d66f0d18843
SHA256:db785a8486fd5f45ef2a56d1d977afa0b445bf4491e1b429a9863c46e5a2d35a
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: taskplanner_maintenance.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/maintenance/taskplanner_maintenance.js
MD5: c4330ed5aced8829454f0e8893f8725c
SHA1: 178b4ecba1c10e50c162c7e09dc5f4b643303508
SHA256:3ba039d8a74f4fd350441ef7a9f1f98322eb951887ee1635c7d78c66c8908b53
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

taskplanner.zip: taskplanner.jar: textAreaField.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/taskplanner.zip/taskplanner.jar/com/inet/taskplanner/client/js/fields/textAreaField.directive.js
MD5: 46bf6266b3aa8c7d331c34aa58185b2d
SHA1: f6348f31ef689122ec81b2dac2455e15f4b561e6
SHA256:4f679ccc7d9fdb172764575fb3e9fdfbb3cb21d370b3adcf06b17fd7326f877b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

theme.zip: theme.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/theme.zip/theme.jar
MD5: 00ddf561821a77f8c3f6d960710f5b1a
SHA1: 3e551815c7bc9a015cffcc463401ad5f01522c68
SHA256:6f5d14ffd676de679c97bd21feff13e943a6ecd57b0aeec379b5623cbcd108dc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	theme	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	server	Low
Vendor	jar	package name	theme	Low
Vendor	Manifest	built-date	2026-09-28 17:02	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium

Product	file	name	theme	High
Product	jar	package name	server	Low
Product	jar	package name	theme	Highest
Product	jar	package name	theme	Low
Product	Manifest	built-date	2026-09-28 17:02	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	theme	High
Product	Manifest	specification-title	theme	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar
MD5: d7e4d07c1c6ca3966efcf8fd040a03bb
SHA1: b214f00d7ac1722dc02a07bf05e5ce75e78e8aad
SHA256:b5c6f8cac5689d9755d0fbfbb082f1aa8b4129cfb801c4d527df140684f7dff4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	usersandgroupsmanager	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	server	Low
Vendor	jar	package name	usersandgroupsmanager	Low
Vendor	Manifest	built-date	2026-09-28 17:30	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium

Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	usersandgroupsmanager	High
Product	jar	package name	server	Low
Product	jar	package name	usersandgroupsmanager	Highest
Product	jar	package name	usersandgroupsmanager	Low
Product	Manifest	built-date	2026-09-28 17:30	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	usersandgroupsmanager	High
Product	Manifest	specification-title	usersandgroupsmanager	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeAccountSettingsRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeAccountSettingsRenderer.directive.js
MD5: 136a634e0236a238529acf990312d10e
SHA1: 75518847c3c3aa3737e31149c6834bb6c40f4606
SHA256:9901a11fad82515fe2425d4f07163b716e8dfa8233196e7fcdc8f21b3aca6817
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeBooleanRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeBooleanRenderer.directive.js
MD5: e6bb2b0218c39ede42d1779e09d0b306
SHA1: bfedb33d3a2d6896458956fdc4209692d43e0d02
SHA256:7e4281e4831ef87da9cf9e032009349bcf48c35a0b2769e742a978cdda8de750
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeCommaSeparatedRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeCommaSeparatedRenderer.directive.js
MD5: f2b4334af468c4d902238d1bce4da4f3
SHA1: 13237d976be3def9c5fb8515bb13b2eb4f44f9f1
SHA256:ef49de84af5c1d21ff57550ea8cb08de7f2282926acb54a351c841654ce0cfa8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeCurrencyRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeCurrencyRenderer.directive.js
MD5: 576e2e33fecee33b8a52087f7c8f814f
SHA1: 28d72a27ea10bb81cb999030e2da18a830812181
SHA256:fee5d01b210301f4211eca6d318c9a3364ae2f3ca8f43676bd14e4b5b18db3cf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeDateRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeDateRenderer.directive.js
MD5: 5d6dc9ddeeffa4dae40a8db5830a5ffe
SHA1: 3caab689e27efcad78fb231dfe8649b27705a904
SHA256:02070d4104c61c45c621481faa4b93e6ff9e789754422c286432a164a5145eb4
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeDoubleRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeDoubleRenderer.directive.js
MD5: 282c6b2f97252fab8aa8de01cdb7e794
SHA1: d3229fe8d413bb7b85af062729ae1d0fd1802f13

SHA256:02a423eb8b6526660f185e32b27cf9e959e68b5f59d21119389c0605e434df8c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeHintRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeHintRenderer.directive.js
MD5: d0d411e05487c0c9ade80c85c991baa1
SHA1: b4e425ad40fbcbc5666fbae93d2fa6e1bfba2ea1
SHA256:274194771293b6441bbad55ed928e669baab81a5ae9050e0bfb48d5598148991
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeIntegerRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeIntegerRenderer.directive.js
MD5: 7d57b1e45b869cf7c78526578aaf900c
SHA1: ec843905d7355268528f06b659256b0aa7f6691c
SHA256:8201fbe9e0a521a8857e91c5124dd49e5b82d84dfa058cbe5a93bcce69ab99e0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeLinkRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeLinkRenderer.directive.js
MD5: e6c32de54da34adc1552e995eabd9161
SHA1: f4ed38539b7207c87318600525233161a3e044f0
SHA256:844b48b5eb22d782b9f11cc64034bcd18f15727b7d38d727d124831e689d2d31
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeLoginsRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeLoginsRenderer.directive.js
MD5: 77e510f9e074e3104df3096deb39cd91
SHA1: 68e57a5859aa1073fdb62dd1102867d0c7db3c9f
SHA256:70fdfe453166ed5a8bae30f56d71e5e52c58c98db676853519a0d35dd71de650
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeMembersRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeMembersRenderer.directive.js
MD5: 98ed31cd6643d9845db76f33b503a9a6
SHA1: df80ef37e6457c6de831aa7e33c842aad2d4a5d6
SHA256:1764e90680550978e1dafb05dd03d78c03609f5503f66079691924c4f9483800
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeMultilineRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeMultilineRenderer.directive.js
MD5: 6290ca47c8214c96d321b5247250b392
SHA1: ee5f676f9d471da531101d0a0128b45d469b7565
SHA256:6a58b8b83869f39de1f71d80c1cae2576dd143a9a1aa2455bf1989e0ab9aecc1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypePermissionRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypePermissionRenderer.directive.js
MD5: 910b84e42fce52f480e7a26273c0ea1c
SHA1: b040b5343ade8c27562b3787b4a2c47e1819348f
SHA256:ddaba53774a185ab399c5a4c18440d4a93869486552df4a8d53acee382049d73
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeSelectRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeSelectRenderer.directive.js
MD5: 96d7f09370447ddd5aec98e86896001f
SHA1: 42d97ea9de26906450eda22c70d6da2420469c84
SHA256:08aa4784c039f07dd522b3e5a73c8890a71983b4d25409afb6c31b41d8787f42
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeStayLoggedInSessionsRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeStayLoggedInSessionsRenderer.directive.js
MD5: 8f7246a8c4620515a714dd858c7b0847
SHA1: bab49440daa202026ce7fdb25d3c3ab7d0ac2473
SHA256:85a66f84209b323ddf4e87ee26891210234ea42bfc20d6befdc3074cde326595
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeStringListRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeStringListRenderer.directive.js
MD5: 2682f20706afff6c6ad1aee68441b0e3
SHA1: af8ecd34abd5665281ffad86d1297f0f5c77cfb6
SHA256:48a12f6a313566dc062340754b9beaadf809ee89783782f98c7913989b5076cd
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeStringRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeStringRenderer.directive.js
MD5: c6c7e141999112527ac77ca4f395a389
SHA1: 6e51639de8121f9a0ad9543d9ac2ec01a47009d8
SHA256:742eda74339d85e54b5aa9273043e4c0c88923d8ea4f7ee4c7961c65aaf7687e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeTimeRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeTimeRenderer.directive.js
MD5: e834d7ca60ccdd8353523b96a2b452ad
SHA1: c50fe0b63e5ff87973d881b07cd1cb0d9f7e9828
SHA256:f9a97553cc83d22f8d0519cf3fa54db0f9995e490625200af58d138ca72da702
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: fieldtypeTimerangeRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/fieldtypeTimerangeRenderer.directive.js
MD5: 8ca11f921f530ae3c6d14011f1026be2

SHA1: 123f12b6375637b6819435453cbfc089589514d6
SHA256:3e31b81046fd3a24c691fc82c45f4779912d02b3bad3ca52366670c31042edfe
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: membershipentry.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/membershipentry.directive.js
MD5: 84693fc1ef165371ef27b1475ee7408c
SHA1: d49e9b44b5d99f5b63a93dcb031d51aea068ca3c
SHA256:f3fecadbb3c511b7c006eb44006d5203c16f180a1cbb260c756f0b3b670a55d8
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: membershiplist.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/membershiplist.directive.js
MD5: 9de8f2f539c79244aa95473d497004db
SHA1: dab0863017fbaf80d7da94770dbb17d87cff3a80
SHA256:2939b841bcd7d14e9874e99c72e4c0f58e7c8f5b485fe04158782c2b0d3cdcd1
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: nonmembershiplist.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/nonmembershiplist.directive.js
MD5: 22269c6c1e32356a15788a694358c895
SHA1: c4909db34c175ff0621e17f241f66994e0516bc6
SHA256:1f276cac3365d03c06572f9325217ffc7c65db411b5d40035f818c4890e66ffc
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: permissionCheckboxRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/permissionCheckboxRenderer.directive.js
MD5: f43b62e6ec19922b603e65ac0d9811bc
SHA1: b82e36201fade72e6423ba980d5351e13c657bbb
SHA256:e3d32df00dc3c4d43110a9a8f277ce1383c133b6912f0154626190931c6daff7
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: permissionRadiobuttonRenderer.directive.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/renderer/permissionRadiobuttonRenderer.directive.js
MD5: b2674a06f9fcfb8cab9196229817a52c
SHA1: 2816becffb93dad552e07d80fb7e5042e13f1d26
SHA256:07270db8fca85c74ed49ae3f2345692c66443c01ef0be67234cc3d01e0873675
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagercontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagercontroller.js
MD5: 24335cb0d9be21d09bff120058b63245
SHA1: 68e4fed934bf6e8afcad721f3a29f33935227fb8
SHA256:7740ea1e82c96eec8450eb4ce25c66272f820ce5a82059e215fb20477a0a3102
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerdetailscontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerdetailscontroller.js
MD5: c38bf3a2c0ecf9e01ea9ad05d24df149
SHA1: e7814590969d2ba68340def0c5aa86027fe9e543
SHA256:79870f2b184235b7e610014e68b1068e0ac924572a56cc0f0db371a0e5b68883
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerdialogcontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerdialogcontroller.js
MD5: e35a43fa1eb935369c4e018ff1ee7640
SHA1: d239261c725a4ba6e6efa911b48e4909c5372d69
SHA256:3625665593e42ba14b5b40999ac21bdaeaea0baa80831182e221207a5019b541
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerdirectives.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerdirectives.js
MD5: 71705864bf0c0e29da0aaacd463c628d
SHA1: 53abd3000b5a2623f300338103e760d727c5e3e1
SHA256:da8e20cdb85c4b7bbe052c2f29c2dfacdbe726d6e57c81177e3ae5d9ae9dd65b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagereffectivepermissionscontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagereffectivepermissionscontroller.js
MD5: e38beee6d03d93074acba84010e4c176
SHA1: d27284aae10d28fac162196094e0196c7c2486cf
SHA256:c2c9dd56c576d23e8038048090751071a5b29f53bb9fbba03d42cedb31d927d0
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerfactory.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerfactory.js
MD5: d0229309f615f8093828e879fc89f096
SHA1: 069a42cf27fd6eb6d344e6a9e559c3908bf68cc5
SHA256:06a29374dd27a427aed4feab8127de27c780bc26c8e3e4b1b38dd550f993c85b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagermodel.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagermodel.js
MD5: b306da281a8a9a909e3683f0b3fee964
SHA1: d9fecf4ec4baa6ddf11909d794ea2026fc825f1b
SHA256:709abde30057be4d2716d62927646af116a959e0f0f03a0dfe0d8f9505147037
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerpredeletionwarning.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerpredeletionwarning.js
MD5: 2e963c8f1de1c02f2a9c062f03aff6a5

SHA1: 1f5065e679fefcb1e927248cecfd615950df2d1f
SHA256:8cea620f3d0600315b5b8296a91d5b5826093ee4c728d432dd1f00460347aff5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerrenderer.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerrenderer.js
MD5: 4ae8871b0f3b8c3c820998e946f3ae25
SHA1: 529e86d10c63994b8f5bb48270dd481a1df77b5f
SHA256:c96ca7fecfac9f80b8c71fb5ddb835311726c5c5b7a6649941d12317d3feee4e
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagerstatisticscontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagerstatisticscontroller.js
MD5: 15db7d8e1d9c9102dff09a6540eacfdc
SHA1: 0ca6006da11c419453850c3ec9ec855c42e7b58b
SHA256:6d215333ea6f212da404f333e073a3ca4ab48c921f75f159950694913b1b17bf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

usersandgroupsmanager.zip: usersandgroupsmanager.jar: usersandgroupsmanagertakeoutcontroller.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/usersandgroupsmanager.zip/usersandgroupsmanager.jar/com/inet/usersandgroupsmanager/client/js/usersandgroupsmanagertakeoutcontroller.js
MD5: aecb7916c7ddc1ab36bb620e0bba61aa
SHA1: e98561144eeaf1048f88096ef4adeb4de63d971f
SHA256:cdb865f01764972194727fb6a715369b4353c620ecfdbeeadc40021144b7361c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Identifiers

- **None**

webserver.defender.zip: webserver.defender.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.defender.zip/webserver.defender.jar
MD5: 7b294a68eb66396602c9b34eb70b155d
SHA1: 1a01df250b1d37cacc084feb8916ad9d5c24fef4
SHA256:d4d0e6b0a20686caa609582d2097b1c66b8e4e5c32f61d95d0649a1ad17e1b00
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	webserver.defender	High
Vendor	jar	package name	inet	Low

Vendor	jar	package name	webserverdefender	Low
Vendor	Manifest	built-date	2026-09-28 17:41	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	webserver.defender	High
Product	jar	package name	webserverdefender	Low
Product	Manifest	built-date	2026-09-28 17:41	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	webserver.defender	High
Product	Manifest	specification-title	webserver.defender	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

webserver.zip: acme4j-client.jar

Description:

ACME client for Java

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/acme4j-client.jar
MD5: bb6304a381d05fabc95f50d537103c89
SHA1: 8276610d0ee58e66d083b9f749ad997dec5a5c14
SHA256:4a56511512f2e7829dc24fe2a2ca0ac4c6ed593c63b455b36fbdff3044294c2c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence

Vendor	file	name	acme4j-client	High
Vendor	jar	package name	acme4j	Highest
Vendor	jar	package name	shredzone	Highest
Vendor	Manifest	build-jdk-spec	21	Low
Vendor	pom	artifactid	acme4j-client	Low
Vendor	pom	groupid	org.shredzone.acme4j	Highest
Vendor	pom	name	acme4j Client	High
Vendor	pom	parent-artifactid	acme4j	Low
Product	file	name	acme4j-client	High
Product	jar	package name	acme4j	Highest
Product	jar	package name	shredzone	Highest
Product	Manifest	build-jdk-spec	21	Low
Product	pom	artifactid	acme4j-client	Highest
Product	pom	groupid	org.shredzone.acme4j	Highest
Product	pom	name	acme4j Client	High
Product	pom	parent-artifactid	acme4j	Medium
Version	pom	version	5.1.0	Highest

Identifiers

- pkg:maven/org.shredzone.acme4j/acme4j-client@5.1.0 (*Confidence*:High)

webserver.zip: jetty-websocket-core-client.jar

Description:

Jetty Core WebSocket Client Artifact

License:

EPL-2.0 OR Apache-2.0
https://www.eclipse.org/legal/epl-2.0/, https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-websocket-core-client.jar
MD5: ba3cc264c13fbe0db1be7566ae7accf6
SHA1: 58a6d44445c32eef70dad94de5211c2f77ab9112
SHA256:14f2da57077bacdd892fa442d6c76bfbaea51e7771f5ebf35ed6da18b1e5b7bf
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jetty-websocket-core-client	High
Vendor	jar	package name	core	Highest
Vendor	jar	package name	eclipse	Highest
Vendor	jar	package name	jetty	Highest
Vendor	jar	package name	websocket	Highest
Vendor	Manifest	build-jdk-spec	25	Low
Vendor	Manifest	bundle-copyright	Copyright (c) 1995 Mort Bay Consulting Pty Ltd and others.	Low
Vendor	Manifest	bundle-docurl	https://jetty.org/	Low
Vendor	Manifest	bundle-symbolicname	org.eclipse.jetty.websocket.core.client	Medium
Vendor	Manifest	Implementation-Vendor	Eclipse Jetty Project	High
Vendor	Manifest	url	https://jetty.org/	Low
Vendor	pom	artifactid	jetty-websocket-core-client	Low
Vendor	pom	groupid	org.eclipse.jetty.websocket	Highest
Vendor	pom	name	Core :: Websocket :: Client	High
Vendor	pom	parent-artifactid	jetty-websocket	Low
Product	file	name	jetty-websocket-core-client	High
Product	jar	package name	core	Highest
Product	jar	package name	eclipse	Highest
Product	jar	package name	jetty	Highest
Product	jar	package name	websocket	Highest
Product	Manifest	build-jdk-spec	25	Low
Product	Manifest	bundle-copyright	Copyright (c) 1995 Mort Bay Consulting Pty Ltd and others.	Low
Product	Manifest	bundle-docurl	https://jetty.org/	Low
Product	Manifest	Bundle-Name	Core :: Websocket :: Client	Medium
Product	Manifest	bundle-symbolicname	org.eclipse.jetty.websocket.core.client	Medium
Product	Manifest	url	https://jetty.org/	Low
Product	pom	artifactid	jetty-websocket-core-client	Highest
Product	pom	groupid	org.eclipse.jetty.websocket	Highest
Product	pom	name	Core :: Websocket :: Client	High
Product	pom	parent-artifactid	jetty-websocket	Medium
Version	Manifest	Bundle-Version	12.1.12	High

Version	Manifest	Implementation-Version	12.1.12	High
Version	pom	version	12.1.12	Highest

Related Dependencies

- webserver.zip: jetty-client.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-client.jar
  - MD5: 2657827ba402bfe8f3a16a9cd2229a42
  - SHA1: c0cfbdc78ef2724233e476e1c0fbc8fcd8ef4a5b
  - SHA256: d3888e13a893faafda80863c4ef8ea6f9fc3d4a59435997a600407c2d8b2b3d6
  - pkg:maven/org.eclipse.jetty/jetty-client@12.1.12
- webserver.zip: jetty-compression-common.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-compression-common.jar
  - MD5: d3a3775ad64f64bf56c88164bba6334e
  - SHA1: 5b072d5fb3c68f06dab87bdf6148424fdcfca481
  - SHA256: a563077b2d760022fc0de241fec29ebd5b31ed629060235c395b0389f304a148
  - pkg:maven/org.eclipse.jetty.compression/jetty-compression-common@12.1.12
- webserver.zip: jetty-compression-gzip.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-compression-gzip.jar
  - MD5: 38488fe879d1dcd31c81d72aa12073aa
  - SHA1: f34786b7ea7c8eb6949dd359b973f7644147fbd0
  - SHA256: 71315ebfed13187554daaa7fdc41b143f7d3eebdebc8b230b41a96bcb1bc7d04
  - pkg:maven/org.eclipse.jetty.compression/jetty-compression-gzip@12.1.12
- webserver.zip: jetty-ee11-servlet.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-ee11-servlet.jar
  - MD5: c5bf39bd31967bf359bd12afedda00d2
  - SHA1: f034982353d3f37ff98fdc2f4e13c156803d75c3
  - SHA256: af76ee845345f184d96d8f6c926e64f8bda4cf858013598d392ad604d37e6bac
  - pkg:maven/org.eclipse.jetty.ee11/jetty-ee11-servlet@12.1.12
- webserver.zip: jetty-ee11-servlets.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-ee11-servlets.jar
  - MD5: 2fe23745f5f479dcdfb3c24497323bde
  - SHA1: c2526818f0231e74b38f7dc9655a543a1c07149d
  - SHA256: 7f26d302c6bdfff60c24117283073ea24dcda0ad6146038f80ed63aa10f49773
  - pkg:maven/org.eclipse.jetty.ee11/jetty-ee11-servlets@12.1.12
- webserver.zip: jetty-ee11-websocket-jakarta-client.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-ee11-websocket-jakarta-client.jar
  - MD5: 61868844d79b6869ef177c0f6775057a
  - SHA1: cf2a334b6e91b089f672596b58dbc7b8999a25e1
  - SHA256: 68d7f2431989a96e335493a5a18f13106ed5968986c96c0d01d9c882af718b05
  - pkg:maven/org.eclipse.jetty.ee11.websocket/jetty-ee11-websocket-jakarta-client@12.1.12
- webserver.zip: jetty-ee11-websocket-jakarta-common.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-ee11-websocket-jakarta-common.jar
  - MD5: d60512d079ba85b99f3e74674f8f58d2
  - SHA1: 95fab470c24abd2a96879790f56edad1091ded57

        - SHA256: 3df357df1f9370a317c4accd3156046cceab8a7b7f1c952b7d6a4a1dab20db8f
        - pkg:maven/org.eclipse.jetty.ee11.websocket/jetty-ee11-websocket-jakarta-common@12.1.12
    - webserver.zip: jetty-ee11-websocket-servlet.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-ee11-websocket-servlet.jar
        - MD5: c4b20e94eb9bbe508bd5291e407ffaa9
        - SHA1: 33e7936e603ecc193e2abf613acd3da1b545c626
        - SHA256: 0842bedee031daeda081d1f90c9d2508a19124d0551809f1a335eaa93d693e25
        - pkg:maven/org.eclipse.jetty.ee11.websocket/jetty-ee11-websocket-servlet@12.1.12
    - webserver.zip: jetty-http.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-http.jar
        - MD5: dc7377b12dd40b471772ce93edee1f95
        - SHA1: 18e79d9da43b31fe7004621f5dbf4ba92b9edd19
        - SHA256: 5476e16ef7e28883dba3669ee06491021e4a9aeba9a76f901a3f5c2bb5252a3e
        - pkg:maven/org.eclipse.jetty/jetty-http@12.1.12
    - webserver.zip: jetty-http2-common.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-http2-common.jar
        - MD5: d6c12f64750a9e6879c26daf9121e2ec
        - SHA1: ccd7ab35b0db5d2e64c42c78311179b5ba00e52e
        - SHA256: 31c4e73da6a83e6b77531aa9a2aa8e8b64265512672b7db18476872b01b22acd
        - pkg:maven/org.eclipse.jetty.http2/jetty-http2-common@12.1.12
    - webserver.zip: jetty-http2-hpack.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-http2-hpack.jar
        - MD5: f78ee65e8e21fbe456fcc5aeea330617
        - SHA1: cb7d1d1785460729d437bf4019e971a7ceec12b2
        - SHA256: b59a90111b03359a18a499a5b21b83555a1990ed26df01dc15d477e6800c8674
        - pkg:maven/org.eclipse.jetty.http2/jetty-http2-hpack@12.1.12
    - webserver.zip: jetty-io.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-io.jar
        - MD5: a8f5eb6234948453ec1a7cfcaa782fec
        - SHA1: 99703c1359bc6114b30fefdd0fa6db2fa26355f5
        - SHA256: a809a6a534adccfaa08bca94aa54328e3ac858973ccddbda770f7e9e0f5099fc
        - pkg:maven/org.eclipse.jetty/jetty-io@12.1.12
    - webserver.zip: jetty-security.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-security.jar
        - MD5: 02140347c194c3a8fd60dba0967d857a
        - SHA1: 336bf8d287b649400d9fad16ecf39593b17b23a4
        - SHA256: fcc0206c1ac66b632ef29a59ccf76c3f3737a62ef54694b1d111eeb2e6efe804
        - pkg:maven/org.eclipse.jetty/jetty-security@12.1.12
    - webserver.zip: jetty-session.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-session.jar
        - MD5: 2352895ffab6e38c7b8c14cb5b25d68f
        - SHA1: df924fc0f60f96b6acd1cd267c24c8679f10ffea
        - SHA256: 73aea4cdd91f2027da1a09cd5953b661625017971d53d8e1ff342f8547752b06
        - pkg:maven/org.eclipse.jetty/jetty-session@12.1.12
    - webserver.zip: jetty-util.jar
        - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-util.jar
        - MD5: db0ce60e5e65b6cece5c9c8b01c0f7fa

- SHA1: 1f6c7ee04775b812ebf35cbea57abecbd6c70903
- SHA256: f6fbfa61cfcca032ff82ad8ff3b66a14374047f15486521dbc89a6c0df19ccf2
- pkg:maven/org.eclipse.jetty/jetty-util@12.1.12

- webserver.zip: jetty-websocket-core-common.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-websocket-core-common.jar
  - MD5: 5c5779cbf4359aaed394e9101abfbbc9
  - SHA1: 07b17a921a090495e0dc86f82bbff0cf8e9af466
  - SHA256: a1ef0c79a4b8b9e4ce969e70d8de9fbed4776625863bdbd5eb5f69fb70208399
  - pkg:maven/org.eclipse.jetty.websocket/jetty-websocket-core-common@12.1.12
- webserver.zip: jetty-websocket-jetty-api.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-websocket-jetty-api.jar
  - MD5: 07535d16dec790d76b5072e502a7cc3d
  - SHA1: 014cb6ada7d514f8818868c88898f04343642f36
  - SHA256: 887090638bf758dce9268478a3ccf168929de52dcdecdddb4eaff62263cbd961
  - pkg:maven/org.eclipse.jetty.websocket/jetty-websocket-jetty-api@12.1.12

Identifiers

- pkg:maven/org.eclipse.jetty.websocket/jetty-websocket-core-client@12.1.12 (*Confidence*:High)
- cpe:2.3:a:eclipse:jetty:12.1.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:jetty:jetty:12.1.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:mortbay_jetty:jetty:12.1.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

webserver.zip: jetty-websocket-core-server.jar

Description:

Jetty Core WebSocket Server Artifact

License:

EPL-2.0 OR Apache-2.0
https://www.eclipse.org/legal/epl-2.0/, https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jetty-websocket-core-server.jar
MD5: 22b2d27cf87fc59fc3dfb822c26161ec
SHA1: dfc760fe022a18b7f227ba3552a9a7494afdda34
SHA256:d91becae70e7b15e6200f40d02239d8315f8b26c90d4ab38348fcdad41c0ebf5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jetty-websocket-core-server	High
Vendor	jar	package name	core	Highest

Vendor	jar	package name	eclipse	Highest
Vendor	jar	package name	jetty	Highest
Vendor	jar	package name	websocket	Highest
Vendor	Manifest	build-jdk-spec	25	Low
Vendor	Manifest	bundle-copyright	Copyright (c) 1995 Mort Bay Consulting Pty Ltd and others.	Low
Vendor	Manifest	bundle-docurl	https://jetty.org/	Low
Vendor	Manifest	bundle-symbolicname	org.eclipse.jetty.websocket.core.server	Medium
Vendor	Manifest	Implementation-Vendor	Eclipse Jetty Project	High
Vendor	Manifest	url	https://jetty.org/	Low
Vendor	pom	artifactid	jetty-websocket-core-server	Low
Vendor	pom	groupid	org.eclipse.jetty.websocket	Highest
Vendor	pom	name	Core :: Websocket :: Server	High
Vendor	pom	parent-artifactid	jetty-websocket	Low
Product	file	name	jetty-websocket-core-server	High
Product	jar	package name	core	Highest
Product	jar	package name	eclipse	Highest
Product	jar	package name	jetty	Highest
Product	jar	package name	websocket	Highest
Product	Manifest	build-jdk-spec	25	Low
Product	Manifest	bundle-copyright	Copyright (c) 1995 Mort Bay Consulting Pty Ltd and others.	Low
Product	Manifest	bundle-docurl	https://jetty.org/	Low
Product	Manifest	Bundle-Name	Core :: Websocket :: Server	Medium
Product	Manifest	bundle-symbolicname	org.eclipse.jetty.websocket.core.server	Medium
Product	Manifest	url	https://jetty.org/	Low
Product	pom	artifactid	jetty-websocket-core-server	Highest
Product	pom	groupid	org.eclipse.jetty.websocket	Highest
Product	pom	name	Core :: Websocket :: Server	High
Product	pom	parent-artifactid	jetty-websocket	Medium
Version	Manifest	Bundle-Version	12.1.12	High
Version	Manifest	Implementation-Version	12.1.12	High
Version	pom	version	12.1.12	Highest

Related Dependencies

- webserver.zip: jetty-alpn-java-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-alpn-java-server.jar
  - MD5: 608ef9e6596233c0764ba4af63b7df63
  - SHA1: 52cc7532d554a57a9a59831a6430624e851818b8
  - SHA256: 47ada2ed59a9ec10f56837f08e2ed086c148dd4b7cd3ba9ceab1b9ee0f985518
  - pkg:maven/org.eclipse.jetty/jetty-alpn-java-server@12.1.12
- webserver.zip: jetty-alpn-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-alpn-server.jar
  - MD5: 82297067eee3cf0b1d74b4e12fbd647d
  - SHA1: 8356e9fa99b733d5522620dbb7063f8fed3f5c27
  - SHA256: 48c84d4e7723218c61c5c9849b558319401e3cd6333cd5c85c0ec2391402c51f
  - pkg:maven/org.eclipse.jetty/jetty-alpn-server@12.1.12
- webserver.zip: jetty-compression-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-compression-server.jar
  - MD5: 40f794823ac9dae977c7ac49b31ea356
  - SHA1: f3ef25eff215e611a396b46d980a30c5a465f373
  - SHA256: af8d98f91c18a08c1adf21e75512fc570a372896c07245c73d8f257c59e6f9f0
  - pkg:maven/org.eclipse.jetty.compression/jetty-compression-server@12.1.12
- webserver.zip: jetty-ee11-websocket-jakarta-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-ee11-websocket-jakarta-server.jar
  - MD5: ba2d2f437c927d927151bff86c994df9
  - SHA1: 4275494c910a658d9cbaf08eba9a23947e4ff28b
  - SHA256: 008e85ee0a1470a547841c5e20682b90e763f073cf4198d4a3d34c1706b698d7
  - pkg:maven/org.eclipse.jetty.ee11.websocket/jetty-ee11-websocket-jakarta-server@12.1.12
- webserver.zip: jetty-ee11-websocket-jetty-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-ee11-websocket-jetty-server.jar
  - MD5: 7402bebdc3b6e158c2c564602d398c8c
  - SHA1: 378037b4f183b1d13b0f385ab2f45d5abd7a7525
  - SHA256: efff205f329aee83cb1656339f6914700ee9ed21b46a0fef236031c128d0d2d9
  - pkg:maven/org.eclipse.jetty.ee11.websocket/jetty-ee11-websocket-jetty-server@12.1.12
- webserver.zip: jetty-http2-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-http2-server.jar
  - MD5: 1fa1e7c63de9b5a8a1b8c27f39c77464
  - SHA1: b6ccd9a4ff9b49745c62a3dadc4c461f541b3a3d
  - SHA256: e84feb7c6bd11c3a49b0a60a9a37ade908677ae8fceb056e3ae2f3b907ebed3f
  - pkg:maven/org.eclipse.jetty.http2/jetty-http2-server@12.1.12
- webserver.zip: jetty-server.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins /webserver.zip/jetty-server.jar
  - MD5: fc41363ef58a4184571c2a7e24b52975
  - SHA1: ff303f5274bf4f9ba91588de595ce8689cb1f34c
  - SHA256: 9ba04bb8d011444a10873a51b1cb8297c04f70db55c8a8d9efcc3a9b97896787
  - pkg:maven/org.eclipse.jetty/jetty-server@12.1.12

Identifiers

- pkg:maven/org.eclipse.jetty.websocket/jetty-websocket-core-server@12.1.12 (*Confidence*:High)
- cpe:2.3:a:eclipse:jetty:12.1.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:jetty:jetty:12.1.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:jetty:jetty_http_server:12.1.12:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:mortbay_jetty:jetty:12.1.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

webserver.zip: jose4j.jar

Description:

The jose.4.j library is a robust and easy to use open source implementation of JSON Web Token (JWT) and the JOSE specification suite (JWS, JWE, and JWK).
It is written in Java and relies solely on the JCA APIs for cryptography.
Please see https://bitbucket.org/b_c/jose4j/wiki/Home for more info, examples, etc..

License:

The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/jose4j.jar
MD5: f57cb91efc5beaa940029f5515a888c2
SHA1: 357a3836bb5da16f314f3a1e954518e5468cd915
SHA256:7314af50cde9c99e8eaf43eee617a23edcc6bb4303622106435509499d837ef
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jose4j	High
Vendor	jar	package name	jca	Highest
Vendor	jar	package name	jose4j	Highest
Vendor	jar	package name	json	Highest
Vendor	jar	package name	jwe	Highest
Vendor	jar	package name	jwk	Highest
Vendor	jar	package name	jws	Highest
Vendor	jar	package name	jwt	Highest
Vendor	jar	package name	use	Highest
Vendor	Manifest	automatic-module-name	org.jose4j	Medium
Vendor	Manifest	bundle-	org.bitbucket.b_c.jose4j	Medium

		symbolicname		
Vendor	pom	artifactid	jose4j	Low
Vendor	pom	developer email	brian.d.campbell@gmail.com	Low
Vendor	pom	developer name	Brian Campbell	Medium
Vendor	pom	groupid	org.bitbucket.b_c	Highest
Vendor	pom	name	jose4j	High
Vendor	pom	url	https://bitbucket.org/b_c/jose4j/	Highest
Product	file	name	jose4j	High
Product	jar	package name	jca	Highest
Product	jar	package name	jose4j	Highest
Product	jar	package name	json	Highest
Product	jar	package name	jwe	Highest
Product	jar	package name	jwk	Highest
Product	jar	package name	jws	Highest
Product	jar	package name	jwt	Highest
Product	jar	package name	use	Highest
Product	Manifest	automatic-module-name	org.jose4j	Medium
Product	Manifest	Bundle-Name	jose4j	Medium
Product	Manifest	bundle-symbolicname	org.bitbucket.b_c.jose4j	Medium
Product	pom	artifactid	jose4j	Highest
Product	pom	developer email	brian.d.campbell@gmail.com	Low
Product	pom	developer name	Brian Campbell	Low
Product	pom	groupid	org.bitbucket.b_c	Highest
Product	pom	name	jose4j	High
Product	pom	url	https://bitbucket.org/b_c/jose4j/	Medium
Version	Manifest	Bundle-Version	0.9.6	High
Version	pom	version	0.9.6	Highest

Identifiers

- pkg:maven/org.bitbucket.b_c/jose4j@0.9.6 (*Confidence*:High)
- cpe:2.3:a:jose4j_project:jose4j:0.9.6:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

webserver.zip: webserver.jar

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/webserver.zip/webserver.jar
MD5: f78dcfd62332f2b13a10de46ea709009
SHA1: 7bbd70617bc55a427834b13cc0b9f9c6c4a7ca98
SHA256:98cabfa6f5e14fef4244f57108faf3e677e6f0e5856533f10d9dffa2d0b89294
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	webserver	High
Vendor	jar	package name	inet	Low
Vendor	jar	package name	webserver	Low
Vendor	Manifest	built-date	2026-09-28 17:17	Low
Vendor	Manifest	implementation-group	shared	Low
Vendor	Manifest	Implementation-Vendor	i-net software	High
Vendor	Manifest	Implementation-Vendor-Id	de.inetsoftware	Medium
Vendor	Manifest	specification-vendor	i-net software	Low
Vendor	Manifest	vendor	i-net software GmbH, Berlin, Germany	Medium
Product	file	name	webserver	High
Product	jar	package name	webserver	Highest
Product	jar	package name	webserver	Low
Product	Manifest	built-date	2026-09-28 17:17	Low
Product	Manifest	implementation-group	shared	Low
Product	Manifest	Implementation-Title	webserver	High
Product	Manifest	specification-title	webserver	Medium
Version	Manifest	Implementation-Version	26.10.199	High

Identifiers

- **None**

Suppressed Vulnerabilities

authentication.pam.zip: jna.jar

Description:

JNA Library

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/jna.jar
MD5: 97fcb12698f8c1e4eed897e5c490e098
SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jna	High
Vendor	jar	package name	jna	Highest
Vendor	jar	package name	jna	Low
Vendor	jar	package name	sun	Highest
Vendor	jar	package name	sun	Low
Vendor	jar (hint)	package name	oracle	Highest
Vendor	jar (hint)	package name	oracle	Low
Vendor	Manifest	automatic-module-name	com.sun.jna	Medium
Vendor	Manifest	bundle-activationpolicy	lazy	Low
Vendor	Manifest	bundle-category	jni	Low
Vendor	Manifest	bundle-nativecode	com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win32, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win32, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64;osname=win32, com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64;osname=win, com/sun/jna/w32ce-arm/jnidispatch.dll; processor=arm;osname=wince, com/sun/jna/sunos-x86/libjnidispatch.so; processor=x86;osname=sunos, com/sun/jna/sunos-x86-64/libjnidispatch.so; processor=x86-64;osname=sunos, com/sun/jna/sunos-sparc/libjnidispatch.so; processor=sparc;osname=sunos, com/sun/jna/sunos-sparcv9/libjnidispatch.so; processor=sparcv9;	Low

			osname=sunos, com/sun/jna/aix-ppc /libjnidispatch.a; processor=ppc; osname=aix, com/sun/jna/aix-ppc64 /libjnidispatch.a; processor=ppc64; osname=aix, com/sun/jna/linux-ppc /libjnidispatch.so; processor=ppc; osname=linux, com/sun/jna/linux-ppc64 /libjnidispatch.so; processor=ppc64; osname=linux, com/sun/jna/linux-ppc64le /libjnidispatch.so; processor=ppc64le; osname=linux, com/sun/jna/linux-x86 /libjnidispatch.so; processor=x86; osname=linux, com/sun/jna/linux-x86-64 /libjnidispatch.so; processor=x86-64; osname=linux, com/sun/jna/linux-arm /libjnidispatch.so; processor=arm; osname=linux, com/sun/jna/linux-arm /libjnidispatch.so; processor=arm_le; osname=linux, com/sun/jna/linux-armel /libjnidispatch.so; processor=armel; osname=linux, com/sun/jna/linux-aarch64 /libjnidispatch.so; processor=aarch64; osname=linux, com/sun/jna/linux-ia64 /libjnidispatch.so; processor=ia64; osname=linux, com/sun/jna/linux-sparcv9 /libjnidispatch.so; processor=sparcv9; osname=linux, com/sun/jna/linux-mips64el /libjnidispatch.so; processor=mips64el; osname=linux, com/sun/jna/linux-s390x /libjnidispatch.so; processor=S390x; osname=linux, com/sun/jna/linux-loongarch64/libjnidispatch.so; processor=loongarch64;osname=linux, com /sun/jna/linux-riscv64/libjnidispatch.so; processor=riscv64;osname=linux, com/sun /jna/dragonflybsd-x86-64/libjnidispatch.so; processor=x86-64;osname=dragonflybsd, com/sun/jna/freebsd-x86/libjnidispatch.so; processor=x86;osname=freebsd, com/sun /jna/freebsd-x86-64/libjnidispatch.so; processor=x86-64;osname=freebsd, com /sun/jna/freebsd-aarch64/libjnidispatch.so; processor=aarch64;osname=freebsd, com /sun/jna/freebsd-ppc64le/libjnidispatch.so; processor=ppc64le;osname=freebsd, com /sun/jna/freebsd-ppc64/libjnidispatch.so; processor=ppc64;osname=freebsd, com/sun /jna/openbsd-x86/libjnidispatch.so; processor=x86;osname=openbsd, com/sun /jna/openbsd-x86-64/libjnidispatch.so; processor=x86-64;osname=openbsd, com /sun/jna/darwin-ppc/libjnidispatch.jnilib; osname=macosx;processor=ppc, com/sun /jna/darwin-ppc64/libjnidispatch.jnilib; osname=macosx;processor=ppc64, com/sun /jna/darwin-x86/libjnidispatch.jnilib; osname=macosx;processor=x86, com/sun /jna/darwin-x86-64/libjnidispatch.jnilib; osname=macosx;processor=x86-64, com /sun/jna/darwin-aarch64/libjnidispatch.jnilib; osname=macosx;processor=aarch64	
Vendor	Manifest	bundle-requiredexecution	JavaSE-1.6	Low
Vendor	Manifest	bundle-symbolicname	com.sun.jna	Medium

Vendor	Manifest	Implementation-Vendor	JNA Development Team	High
Vendor	Manifest	specification-vendor	JNA Development Team	Low
Product	file	name	jna	High
Product	jar	package name	jna	Highest
Product	jar	package name	jna	Low
Product	jar	package name	library	Highest
Product	jar	package name	native	Highest
Product	jar	package name	sun	Highest
Product	jar	package name	win32	Highest
Product	Manifest	automatic-module-name	com.sun.jna	Medium
Product	Manifest	bundle-activationpolicy	lazy	Low
Product	Manifest	bundle-category	jni	Low
Product	Manifest	Bundle-Name	jna	Medium
Product	Manifest	bundle-nativecode	com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win32, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win32, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64; osname=win32, com/sun/jna/win32-x86/jnidispatch.dll; processor=x86;osname=win, com/sun/jna/win32-x86-64/jnidispatch.dll; processor=x86-64;osname=win, com/sun/jna/win32-aarch64/jnidispatch.dll; processor=aarch64;osname=win, com/sun/jna/w32ce-arm/jnidispatch.dll; processor=arm;osname=wince, com/sun/jna/sunos-x86/libjnidispatch.so; processor=x86; osname=sunos, com/sun/jna/sunos-x86-64/libjnidispatch.so; processor=x86-64; osname=sunos, com/sun/jna/sunos-sparc/libjnidispatch.so; processor=sparc; osname=sunos, com/sun/jna/sunos-sparcv9/libjnidispatch.so; processor=sparcv9; osname=sunos, com/sun/jna/aix-ppc/libjnidispatch.a; processor=ppc; osname=aix, com/sun/jna/aix-ppc64/libjnidispatch.a; processor=ppc64; osname=aix, com/sun/jna/linux-ppc/libjnidispatch.so; processor=ppc; osname=linux, com/sun/jna/linux-ppc64/libjnidispatch.so; processor=ppc64; osname=linux, com/sun/jna/linux-ppc64le/libjnidispatch.so; processor=ppc64le; osname=linux, com/sun/jna/linux-x86/libjnidispatch.so; processor=x86; osname=linux, com/sun/jna/linux-x86-64/libjnidispatch.so; processor=x86-64; osname=linux, com/sun/jna/linux-arm/libjnidispatch.so; processor=arm; osname=linux, com/sun/jna/linux-arm/libjnidispatch.so; processor=arm_le; osname=linux, com/sun/jna/linux-armel	Low

			/libjnidispatch.so; processor=armel; osname=linux, com/sun/jna/linux-aarch64 /libjnidispatch.so; processor=aarch64; osname=linux, com/sun/jna/linux-ia64 /libjnidispatch.so; processor=ia64; osname=linux, com/sun/jna/linux-sparcv9 /libjnidispatch.so; processor=sparcv9; osname=linux, com/sun/jna/linux-mips64el /libjnidispatch.so; processor=mips64el; osname=linux, com/sun/jna/linux-s390x /libjnidispatch.so; processor=S390x; osname=linux, com/sun/jna/linux-loongarch64/libjnidispatch.so; processor=loongarch64;osname=linux, com /sun/jna/linux-riscv64/libjnidispatch.so; processor=riscv64;osname=linux, com/sun /jna/dragonflybsd-x86-64/libjnidispatch.so; processor=x86-64;osname=dragonflybsd, com/sun/jna/freebsd-x86/libjnidispatch.so; processor=x86;osname=freebsd, com/sun /jna/freebsd-x86-64/libjnidispatch.so; processor=x86-64;osname=freebsd, com /sun/jna/freebsd-aarch64/libjnidispatch.so; processor=aarch64;osname=freebsd, com /sun/jna/freebsd-ppc64le/libjnidispatch.so; processor=ppc64le;osname=freebsd, com /sun/jna/freebsd-ppc64/libjnidispatch.so; processor=ppc64;osname=freebsd, com/sun /jna/openbsd-x86/libjnidispatch.so; processor=x86;osname=openbsd, com/sun /jna/openbsd-x86-64/libjnidispatch.so; processor=x86-64;osname=openbsd, com /sun/jna/darwin-ppc/libjnidispatch.jnilib; osname=macosx;processor=ppc, com/sun /jna/darwin-ppc64/libjnidispatch.jnilib; osname=macosx;processor=ppc64, com/sun /jna/darwin-x86/libjnidispatch.jnilib; osname=macosx;processor=x86, com/sun /jna/darwin-x86-64/libjnidispatch.jnilib; osname=macosx;processor=x86-64, com /sun/jna/darwin-aarch64/libjnidispatch.jnilib; osname=macosx;processor=aarch64	
Product	Manifest	bundle-requiredexecution	JavaSE-1.6	Low
Product	Manifest	bundle-symbolicname	com.sun.jna	Medium
Product	Manifest	Implementation-Title	com.sun.jna	High
Product	Manifest	specification-title	Java Native Access (JNA)	Medium
Version	jar	package name	jna	Highest
Version	jar	package name	sun	Highest
Version	jar	package name	win32	Highest
Version	Manifest	Bundle-Version	5.18.1	High
Version	Manifest	Implementation-Version	5.18.1 (b0)	High

Related Dependencies

- authentication.windows.zip: jna.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.windows.zip/jna.jar
  - MD5: 97fcb12698f8c1e4eed897e5c490e098
  - SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
  - SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2
- cowork.calls.zip: jna.jar
  - File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jna.jar
  - MD5: 97fcb12698f8c1e4eed897e5c490e098
  - SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
  - SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2009-2476 suppressed

The Java Management Extensions (JMX) implementation in Sun Java SE 6 before Update 15, and OpenJDK, does not properly enforce OpenType checks, which allows context-dependent attackers to bypass intended access restrictions by leveraging finalizer resurrection to obtain a reference to a privileged object.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513220
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10381
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html

- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- secalert@redhat.com - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- secalert@redhat.com - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- secalert@redhat.com - http://secunia.com/advisories/37386
- secalert@redhat.com - http://security.gentoo.org/glsa/glsa-200911-02.xml
- secalert@redhat.com - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- secalert@redhat.com - http://www.vupen.com/english/advisories/2009/2543
- secalert@redhat.com - https://bugzilla.redhat.com/show_bug.cgi?id=513220
- secalert@redhat.com - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10381
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- secalert@redhat.com - PATCH,VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...
- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- cpe:2.3:a:sun:openjdk:*:*:*:*:*:*:*:*

CVE-2009-2689 suppressed

JDK13Services.getProviders in Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, grants full privileges to instances of unspecified object types, which allows context-dependent attackers to bypass intended access restrictions via an untrusted (1) applet or (2) application.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://java.sun.com/javase/6/webnotes/6u15.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml

- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513222
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9603
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://java.sun.com/javase/6/webnotes/6u15.html
- cve@mitre.org - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/2543
- cve@mitre.org - https://bugzilla.redhat.com/show_bug.cgi?id=513222
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9603
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...
- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- cpe:2.3:a:sun:java_se:*:20:*:*:*:*:*:* versions up to (including) 5.0
- cpe:2.3:a:sun:openjdk:*:*:*:*:*:*:*:*

CVE-2009-2475 suppressed

Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, might allow context-dependent attackers to obtain sensitive information via vectors involving static variables that are declared without the final keyword, related to (1) LayoutQueue, (2) Cursor.predefined, (3) AccessibleResourceBundle.getContents, (4) ImageReaderSpi.STANDARD_INPUT_TYPE, (5) ImageWriterSpi.STANDARD_OUTPUT_TYPE, (6) the imageio plugins, (7) DnsContext.debug, (8) RmfFileReader/StandardMidiFileWriter.types, (9) AbstractSaslImpl.logger, (10) Synth.Region.uiToRegionMap/lowerCaseNameMap, (11) the Introspector class and a cache of BeanInfo, and (12) JAX-WS, a different vulnerability than CVE-2009-2673.

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: /AV:N/AC:L/Au:N/C:C/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://java.sun.com/javase/6/webnotes/6u15.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513215
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10221
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- secalert@redhat.com - http://java.sun.com/javase/6/webnotes/6u15.html
- secalert@redhat.com - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- secalert@redhat.com - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- secalert@redhat.com - http://secunia.com/advisories/37386
- secalert@redhat.com - http://security.gentoo.org/glsa/glsa-200911-02.xml
- secalert@redhat.com - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- secalert@redhat.com - http://www.vupen.com/english/advisories/2009/2543
- secalert@redhat.com - https://bugzilla.redhat.com/show_bug.cgi?id=513215
- secalert@redhat.com - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10221
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- secalert@redhat.com - PATCH
- secalert@redhat.com - PATCH,VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...
- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- cpe:2.3:a:sun:java_se:*:20:*:*:*:*:*:* versions up to (including) 5.0
- cpe:2.3:a:sun:openjdk:*:*:*:*:*:*:*:*

CVE-2009-2716 suppressed

The plugin functionality in Sun Java SE 6 before Update 15 does not properly implement version selection, which allows context-dependent attackers to leverage vulnerabilities in "old zip and certificate handling" and have unspecified other impact via unknown vectors.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2676 suppressed

Unspecified vulnerability in JNLPAppletlauncher in Sun Java SE, and SE for Business, in JDK and JRE 6 Update 14 and earlier and JDK and JRE 5.0 Update 19 and earlier; and Java SE for Business in SDK and JRE 1.4.2_21 and earlier; allows remote attackers to create or modify arbitrary files via vectors involving an untrusted Java applet that accesses an old version of JNLPAppletLauncher.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00003.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
- af854a3a-2127-422b-91ae-364da2661108 - http://marc.info/?l=bugtraq&m=125787273209737&w=2
- af854a3a-2127-422b-91ae-364da2661108 - http://osvdb.org/56789
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/bid/35946
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securitytracker.com/id?1022657
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A8453
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - US_GOVERNMENT_RESOURCE
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00003.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
- cve@mitre.org - http://marc.info/?l=bugtraq&m=125787273209737&w=2
- cve@mitre.org - http://osvdb.org/56789
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.securityfocus.com/bid/35946
- cve@mitre.org - http://www.securitytracker.com/id?1022657
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A8453
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH,VENDOR_ADVISORY
- cve@mitre.org - US_GOVERNMENT_RESOURCE
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:*:*:*:*:*:*:*
- ...
- cpe:2.3:a:sun:java_se:*:*:*:*:*:*:*:*

- cpe:2.3:a:sun:java_se:*:*:business:*:*:*:*:*
- cpe:2.3:a:sun:jdk:*:update19:*:*:*:*:*:* versions up to (including) 1.5.0
- cpe:2.3:a:sun:jdk:*:update_14:*:*:*:*:*:* versions up to (including) 1.6.0
- cpe:2.3:a:sun:jdk:1.5.0:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update1:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update10:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update11:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update11_b03:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update12:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update13:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update14:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update15:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update16:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update17:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update18:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update2:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update3:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update4:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update5:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update6:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update7:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update8:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.5.0:update9:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update1:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update2:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_10:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_11:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_12:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_13:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_3:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_4:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_5:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_6:*:*:*:*:*:*
- cpe:2.3:a:sun:jdk:1.6.0:update_7:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:*:*:*:*:*:*:*:* versions up to (including) 1.4.2_21
- cpe:2.3:a:sun:jre:*:update19:*:*:*:*:*:* versions up to (including) 1.5.0
- cpe:2.3:a:sun:jre:*:update_14:*:*:*:*:*:* versions up to (including) 1.6.0
- cpe:2.3:a:sun:jre:1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.0_01:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.0_02:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.0_03:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.0_04:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update1:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update2:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update3:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update4:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update5:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update6:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.1:update7:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2:update16:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2:update17:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2:update18:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2:update19:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2:update20:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_1:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_2:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_3:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_4:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_5:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_6:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_7:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_8:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_9:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_10:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_11:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_12:*:*:*:*:*:*:*

- cpe:2.3:a:sun:jre:1.4.2_13:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_14:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.4.2_15:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:*:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update1:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update10:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update11:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update12:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update13:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update14:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update15:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update16:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update17:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update18:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update2:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update3:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update4:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update5:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update6:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update7:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update8:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.5.0:update9:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_1:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_10:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_11:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_12:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_13:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_2:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_3:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_4:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_5:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_6:*:*:*:*:*:*
- cpe:2.3:a:sun:jre:1.6.0:update_7:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:*:*:*:*:*:*:*:* versions up to (including) 1.4.2_21
- cpe:2.3:a:sun:sdk:1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.0_01:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.0_02:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.0_03:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.0_04:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_01:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_02:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_03:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_04:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_05:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_06:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.1_07:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_1:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_2:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_3:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_4:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_5:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_6:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_7:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_8:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_9:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_10:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_11:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_12:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_13:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_14:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_15:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_16:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_17:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_18:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_19:*:*:*:*:*:*:*
- cpe:2.3:a:sun:sdk:1.4.2_20:*:*:*:*:*:*:*

CVE-2009-2717 suppressed

The Abstract Window Toolkit (AWT) implementation in Sun Java SE 6 before Update 15 on Windows 2000 Professional does not provide a Security Warning Icon, which makes it easier for context-dependent attackers to trick a user into interacting unsafely with an untrusted applet.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2690 suppressed

The encoder in Sun Java SE 6 before Update 15, and OpenJDK, grants read access to private variables with unspecified names, which allows context-dependent attackers to obtain sensitive information via an untrusted (1) applet or (2) application.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513223
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9443
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY

- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/2543
- cve@mitre.org - https://bugzilla.redhat.com/show_bug.cgi?id=513223
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9443
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- cve@mitre.org - PATCH
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...
- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- cpe:2.3:a:sun:openjdk:*:*:*:*:*:*:*:*

CVE-2009-2719 suppressed

The Java Web Start implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException) via a crafted .jnlp file, as demonstrated by the jnlp_file/appletDesc/index.html#misc test in the Technology Compatibility Kit (TCK) for the Java Network Launching Protocol (JNLP).

CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2720 suppressed

Unspecified vulnerability in the javax.swing.plaf.synth.SynthContext.isSubregion method in the Swing implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException in the Jemmy library) via unknown vectors.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - PATCH,VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

cowork.calls.zip: ice4j.jar

Description:

A Java implementation of the ICE protocol

License:

Apache-2.0: https://github.com/jitsi/ice4j/blob/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/ice4j.jar
MD5: eaffb973edafb449ec4e38955f96e267
SHA1: da8ec9b9f069da054184c90129c9cdc9078fc7e9
SHA256: dfce847c62008f044edf0f1448bf9c16b5e80de17a0994289a7581e602075532
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	ice4j	High
Vendor	jar	package name	ice	Highest
Vendor	jar	package name	ice4j	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/ice4j	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.ice4j	Medium
Vendor	pom	artifactid	ice4j	Low
Vendor	pom	developer email	dev@jitsi.org	Low
Vendor	pom	developer id	org.jitsi	Medium
Vendor	pom	developer name	Jitsi Team	Medium
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	ice4j	High
Vendor	pom	organization name	jitsi.org	High
Vendor	pom	organization url	https://jitsi.org	Medium
Vendor	pom	url	jitsi/ice4j	Highest
Product	file	name	ice4j	High
Product	jar	package name	ice	Highest
Product	jar	package name	ice4j	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/ice4j	Low
Product	Manifest	Bundle-Name	ice4j	Medium
Product	Manifest	bundle-symbolicname	org.jitsi.ice4j	Medium
Product	pom	artifactid	ice4j	Highest
Product	pom	developer email	dev@jitsi.org	Low
Product	pom	developer id	org.jitsi	Low
Product	pom	developer name	Jitsi Team	Low
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	ice4j	High

Product	pom	organization name	jitsi.org	Low
Product	pom	organization url	https://jitsi.org	Low
Product	pom	url	jitsi/ice4j	High
Version	pom	version	3.2-15-g6da2b08	Highest

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

- cpe:2.3:a:jitsi:jitsi:*:*:*:*:*:*:*:* versions up to (excluding) 2022-09-14

cowork.calls.zip: jicoco-config.jar

Description:

Jitsi Common Components (Configuration Utilities)

License:

"Apache-2.0";link="https://github.com/jitsi/jicoco/blob/master/LICENSE"

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jicoco-config.jar
MD5: 2b360a86dbf02f02173b1e4230e19000
SHA1: 0d026d8cf9582bc707641f68ff979da2f60876d6
SHA256: 40295937ec9471edf7bb8d0602b5363c709638033a01505ead4fa99f27b52550
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jicoco-config	High
Vendor	jar	package name	config	Highest
Vendor	jar	package name	jitsi	Highest
Vendor	Manifest	build-jdk-spec	17	Low
Vendor	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/jicoco/jicoco-config	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.config	Medium
Vendor	pom	artifactid	jicoco-config	Low
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	jicoco-config	High
Vendor	pom	parent-artifactid	jicoco-parent	Low
Product	file	name	jicoco-config	High
Product	jar	package name	config	Highest
Product	jar	package name	jitsi	Highest
Product	Manifest	build-jdk-spec	17	Low
Product	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/jicoco/jicoco-config	Low
Product	Manifest	Bundle-Name	jicoco-config	Medium
Product	Manifest	bundle-symbolicname	org.jitsi.config	Medium
Product	pom	artifactid	jicoco-config	Highest
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	jicoco-config	High

Product	pom	parent-artifactid	jicoco-parent	Medium
Version	pom	version	1.1-178-ga09ed33	Highest

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

- cpe:2.3:a:jitsi:jitsi:*:*:*:*:*:*:*:* versions up to (excluding) 2022-09-14

cowork.calls.zip: jitsi-metaconfig.jar

Description:

jitsi-metaconfig helps solve the problems around the evolution of configuration properties

License:

Apache-2.0: https://github.com/jitsi/jitsi-metaconfig/blob/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-metaconfig.jar
MD5: f41bbbdb0704a947379e648f92de3b6a
SHA1: 2c324f329f52cf28c14236efe18427e0ce7cf411
SHA256: a5f297490bc6797376e7b814e5c23cd548af5a6d5441bce272f0f1abb07abfe2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jitsi-metaconfig	High
Vendor	jar	package name	jitsi	Highest
Vendor	jar	package name	metaconfig	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-metaconfig	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.metaconfig	Medium
Vendor	pom	artifactid	jitsi-metaconfig	Low
Vendor	pom	developer email	dev@jitsi.org	Low
Vendor	pom	developer id	org.jitsi	Medium
Vendor	pom	developer name	Jitsi Team	Medium
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	jitsi-metaconfig	High
Vendor	pom	organization name	jitsi.org	High
Vendor	pom	organization url	https://jitsi.org	Medium
Vendor	pom	url	jitsi/jitsi-metaconfig	Highest
Product	file	name	jitsi-metaconfig	High
Product	jar	package name	jitsi	Highest
Product	jar	package name	metaconfig	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-developers	"org.jitsi";email="dev@jitsi.org";name="Jitsi Team"	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-metaconfig	Low
Product	Manifest	Bundle-Name	jitsi-metaconfig	Medium

Product	Manifest	bundle-symbolicname	org.jitsi.metaconfig	Medium
Product	pom	artifactid	jitsi-metaconfig	Highest
Product	pom	developer email	dev@jitsi.org	Low
Product	pom	developer id	org.jitsi	Low
Product	pom	developer name	Jitsi Team	Low
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	jitsi-metaconfig	High
Product	pom	organization name	jitsi.org	Low
Product	pom	organization url	https://jitsi.org	Low
Product	pom	url	jitsi/jitsi-metaconfig	High
Version	pom	version	1.0-17-g58971d6	Highest

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

- cpe:2.3:a:jitsi:jitsi:*:*:*:*:*:*:*:* versions up to (excluding) 2022-09-14

cowork.calls.zip: jitsi-utils.jar

Description:

A set of basic utilities used in Jitsi projects

License:

Apache-2.0: https://github.com/jitsi/jitsi-utils/blob/master/LICENSE

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-utils.jar
MD5: fa494e8f6b723155f32c3dfb490d8e6e
SHA1: 98b8409c3d8d08aad6a501a32266a669b4252b04
SHA256: aab74933cf6945b99ac3a81d3f27a8753cc3342e97fe522e0b76c18e9ef09923
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	file	name	jitsi-utils	High
Vendor	jar	package name	jitsi	Highest
Vendor	jar	package name	utils	Highest
Vendor	Manifest	build-jdk-spec	11	Low
Vendor	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-utils	Low
Vendor	Manifest	bundle-symbolicname	org.jitsi.utils	Medium
Vendor	pom	artifactid	jitsi-utils	Low
Vendor	pom	developer email	dev@jitsi.org	Low
Vendor	pom	developer id	org.jitsi	Medium
Vendor	pom	developer name	Jitsi Team	Medium
Vendor	pom	groupid	org.jitsi	Highest
Vendor	pom	name	jitsi-utils	High
Vendor	pom	organization name	jitsi.org	High
Vendor	pom	organization url	https://jitsi.org	Medium
Vendor	pom	url	jitsi/jitsi-utils	Highest

Product	file	name	jitsi-utils	High
Product	jar	package name	jitsi	Highest
Product	jar	package name	utils	Highest
Product	Manifest	build-jdk-spec	11	Low
Product	Manifest	bundle-docurl	https://github.com/jitsi/jitsi-utils	Low
Product	Manifest	Bundle-Name	jitsi-utils	Medium
Product	Manifest	bundle-symbolicname	org.jitsi.utils	Medium
Product	pom	artifactid	jitsi-utils	Highest
Product	pom	developer email	dev@jitsi.org	Low
Product	pom	developer id	org.jitsi	Low
Product	pom	developer name	Jitsi Team	Low
Product	pom	groupid	org.jitsi	Highest
Product	pom	name	jitsi-utils	High
Product	pom	organization name	jitsi.org	Low
Product	pom	organization url	https://jitsi.org	Low
Product	pom	url	jitsi/jitsi-utils	High
Version	pom	version	1.0-150-g4ab9a3b	Highest

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-

2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

- cpe:2.3:a:jitsi:jitsi:*:*:*:*:*:*:*:* versions up to (excluding) 2022-09-14

remotegui.zip: angular-animate.jar: angular-animate.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.js
MD5: 31312b87e7226c8bf0714fcef0ea5d18
SHA1: dc9fb55f2c7f922c5ba83449266239ba1353db45
SHA256: 58e79e0e7cbb1e1502d216701e1fae41c405d92320aea1b68a223054096fda93
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in

posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: high

References:
- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617

- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-animate.jar: angular-animate.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.min.js
MD5: 5d2d0f42bb7e1b5503e914674f59dad0
SHA1: 4c15a58541e53c451c6f946d2048104f88b833c7
SHA256: 8e6202b1330a469a61ccdeebbd1cb3a20d0ecdfc8d106f68da5b85e9b67a1cd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-cookies.jar: angular-cookies.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/angular-cookies.js
MD5: e17187aea1f0e6dbd25722e34b754915
SHA1: 20f43f716b9fef7d72537bc1b0e5aa2bc480cee5
SHA256: f3291c552042f6d0c500167769912a78ab3ecec9917128b2d6ea8e7c6714bb97
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-cookies.jar: angular-cookies.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/angular-cookies.min.js
MD5: c41aff8423276d46f0d02de6dcb71524
SHA1: 7dc53f75d5bf7dd2c770cb50f31242c70193c086
SHA256: 926509b494009bea03288bba191a2b238032188e9112377e50fbfe7814c6639b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-sanitize.jar: angular-sanitize.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/angular-sanitize.js
MD5: 0127d7a139abfc8bd45875a9c8ea6348
SHA1: 197aea2acc25a0fa821766400950cac58a3627a5
SHA256: c84c65250afe5a1265f36a7e16c6010652e55c2ae3a779c351fb68536c42bf64
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-sanitize.jar: angular-sanitize.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/angular-sanitize.min.js
MD5: f3c62abeec216e9431e7d5b22d8e813b
SHA1: 21355ef18c5e1ce2b2c711b9dba21cbea0655646
SHA256: cc80a30ad0439c2e9c209b3d7fcffb1d10e6007fd1d00c9cc144f393664a7045
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular.jar: angular.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.js
MD5: e09f650a016c24bc1b5a1edc93bfbade
SHA1: 0f1f7445b761b9bbd5385f9f0b316dbf1ca48696
SHA256: fdca889e76f55fdee7ab661920f37ce19233563bf7f4ac8120f8ebc2ac768768
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular.jar: angular.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.min.js
MD5: 967a32633fa8f38f4ac3376c1a37b992
SHA1: b53b74d8e0b732dcdb98fbe521146b88299ea2f1
SHA256: 396dc1a03d6cc02e9c51a80246e0db53c5c8df9bd07287e3b51bce4a29dab355
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	angularjs	High
Product	RetireJS	name	angularjs	High
Version	RetireJS	version	1.8.3	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:*:*:*:* versions from (including) 1.3.0

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY

- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

CVE-2023-26118 suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY

- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

CVE-2024-8372 suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- info - https://github.com/advisories/GHSA-m9gf-397r-hwpg
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8372

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:
The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here https://docs.angularjs.org/misc/version-support-status .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-4p4w-6hg8-63wx
- info - https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c
- info - https://github.com/advisories/GHSA-4p4w-6hg8-63wx
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-2336
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-2336

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: hugerte.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/hugerte.js
MD5: 608a51d79e72dadae4f71c988978a748
SHA1: f77dd4688fa469741ece9b55f30c07510c83ab1a
SHA256: 9a84cb746a8c0fdd5c857adb90bb4ab0a769335a81246d69224df2decb1bb24b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

DOMPurify before 3.4.12 fails to execute afterSanitizeElements hook for custom elements allowed via CUSTOM_ELEMENT_HANDLING.tagNameCheck, allowing attributes to bypass application security policies. Attackers can preserve sensitive attributes on custom elements that later re-inject them into innerHTML sinks, creating second-order XSS gadgets.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

CVSSv4:
- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.12

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

Unscored:
- Severity: medium

References:
- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: hugerte.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/hugerte.min.js
MD5: 4f869562fbf4bb6f160fb4bf6ec6599f
SHA1: a86e8883ad71949b770498c57966f60ea42518f7

SHA256: be8e43ec41c91e98897e19594c67eeb98fbe269a67cdab2cfb8cb79d298ff05c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

DOMPurify before 3.4.12 fails to execute afterSanitizeElements hook for custom elements allowed via CUSTOM_ELEMENT_HANDLING.tagNameCheck, allowing attributes to bypass application security policies. Attackers can preserve sensitive attributes on custom elements that later re-inject them into innerHTML sinks, creating second-order XSS gadgets.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

CVSSv4:
- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.12

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: theme.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/theme.js
MD5: cf817d8941a3c0111193ece2d7c9b929
SHA1: f7a71244e44dcbf90a9804051bd788b293289a8e
SHA256: 8e0f595de763e6ede53566f5516c6744a175fabd46c40ba3cba6ed39140bb926
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

DOMPurify before 3.4.12 fails to execute afterSanitizeElements hook for custom elements allowed via CUSTOM_ELEMENT_HANDLING.tagNameCheck, allowing attributes to bypass application security policies. Attackers can preserve sensitive attributes on custom elements that later re-inject them into innerHTML sinks, creating second-order XSS gadgets.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

CVSSv4:

- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.12

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: theme.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/theme.min.js
MD5: 8bf8c393660a3656dc0e4b9f12bdc697
SHA1: 49a25ecc5db9c1e0f63804f3ab89885d7d0119f9
SHA256: a43e3e8ec4abb5adff7d91c3c7fe12323920c7bccbcd47ba84625353a012d513
Referenced In Project/Scope: CoWorkInstaller

Evidence

Type	Source	Name	Value	Confidence
Vendor	RetireJS	name	DOMPurify	High
Product	RetireJS	name	DOMPurify	High
Version	RetireJS	version	3.4.11	High

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

DOMPurify before 3.4.12 fails to execute afterSanitizeElements hook for custom elements allowed via CUSTOM_ELEMENT_HANDLING.tagNameCheck, allowing attributes to bypass application security policies. Attackers can preserve sensitive attributes on custom elements that later re-inject them into innerHTML sinks, creating second-order XSS gadgets.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

CVSSv4:
- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.12

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

Notes: HugeRTE: There is currently no fixed date. https://github.com/hugerte/hugerte/issues/206

Unscored:
- Severity: medium

References:
- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the CISA Known Exploited Vulnerability Catalog.
This report may contain data retrieved from the Github Advisory Database (via NPM Audit API).
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype Guide OSS Index API.